NORTHROP GRUMMAN
Information Technology

JEDI 2.0
Public Design Review

Agenda

JEDI 2.0 Public Design Review

WEDNESDAY, OCTOBER 29 – JEDI 2.0 WINDOWS PDR

THURSDAY, OCTOBER 30 – JEDI 2.0 SOLARIS PDR

Agenda for Windows Morning

WEDNESDAY, OCTOBER 29

0800-0830 REGISTRATION
0830-0845 CONFERENCE OPENING REMARKS (AFC2ISRC)
0845-0900 JEDI CURRENT PROGRAM STATUS (AFRL)
0900-0915 JEDI WAY AHEAD (AFRL)
0915-0930 JEDI WINDOWS REQUIREMENTS REVIEW (NGIT)
0930-0945 BREAK
0945-1000 JEDI WINDOWS DESIGN OVERVIEW (NGIT)
1000-1030 JEDI WINDOWS INSTALLATION (NGIT)
1030-1100 JEDI WINDOWS JEDI MANAGEMENT CONSOLE (NGIT)
1100-1115 JEDI WINDOWS CLASSIFICATION COMPONENTS (NGIT)
1115-1130 JEDI WINDOWS PASSWORD FILTER (NGIT)
1130-1300 LUNCH

Agenda for Windows Afternoon

WEDNESDAY, OCTOBER 29

1300-1310	JEDI WINDOWS ISD (NGIT)
1310-1320	JEDI WINDOWS WATCHDOG (NGIT)
1330-1340	JEDI WINDOWS PRINT UTILITY (NGIT)
1340-1350	JEDI WINDOWS EVENT BACKUP (NGIT)
1350-1400	JEDI WINDOWS CLEARTEMP (NGIT)
1400-1415	BREAK
1415-1430	JEDI WINDOWS DEADMAN (NGIT)
1430-1445	JEDI WINDOWS LOGON CONSENT (NGIT)
1445-1500	JEDI WINDOWS SECURITY BANNER (NGIT)
1500-1515	JEDI WINDOWS FSD/DEVICELOCK (NGIT)
1515-1530	JEDI WINDOWS RIS/ISS/SUNONE (NGIT)
1530-1545	JEDI WINDOWS WRAPUP/ACTION ITEMS (NGIT)
1545-	JEDI SIDEBAR SESSIONS

Opening Remarks (NGIT)

Objective of this meeting is:

- To present the preliminary design for JEDI 2.0
- Slide presentation of software operation
- Presentation of the GUI look and feel
- To obtain feedback from user representatives regarding design

NORTHROP GRUMMAN
Information Technology

JEDI 2.0
BEGIN PDR

JEDI 2.0 Requirements

- **Improved Print Utility in Windows**
  The existing print utility only works for Postscript printers and is non-intuitive to set up. The system shall have one location for the security configuration and the utility shall be standalone. The utility shall support duplex printing. The utility shall support print servers.
  - Implement print utility based on the native OS functionality
  - The print utility shall utilize existing printer configuration mechanisms in Windows to meet DoDIIS print requirements
  - Support PCL and Postscript printers
  - No manual configurations besides filling in the name, address, organization and classification fields
  - Suppressing banners and classifications will be based on group membership

JEDI 2.0 Requirements

- **Watchdog checking at startup**
  - This utility shall not duplicate Microsoft Functionality. This utility shall send email upon selected service failure
- **Event Backup Scheduler**
  - Event Backup shall allow scheduling of when event backup will pull down the windows audits
  - Will store the host groups, and scheduled event backup settings in the Windows registry
  - Will be able to get a list of the hosts on the network
  - Will be able to list what backups are currently scheduled
  - Will be able to cancel currently scheduled event backups
  - Will allow the user to specify the location that event backups will be archived
  - Will function properly over terminal services

JEDI 2.0 Requirements

- **Event Backup - Log Types**
  - Event Backup shall pull System, Application, and custom logs in addition to the current capability of pulling the Security logs
  - The Event Backup Scheduler shall be able to find the locations of custom logs through examination of the Windows registry
- **Event Backup - Pulling Audits**
  - Event Backup shall provide a mechanism for on demand downloading of the audits
  - Will allow on demand downloads of logs for all hosts, selected hosts, or selected groups of hosts
- **Event Backup - Log Errors**
  - Event Backup shall log errors to the Windows Application Log Files
  - Event Backup and the Event Backup Scheduler shall have a mechanism for writing to log files
  - Will have meaningful exit codes to indicate to the Event Backup Scheduler GUI whether or not an on demand download was successful

JEDI 2.0 Requirements

- **Event Backup**
  - JEDI shall create an MMC plug-in to configure the event backup functionality
  - The on demand GUI shall be part of the Event Backup Scheduler MMC plug-in
  - The user shall be able to enter a event backup username and password as part of the installation. The user shall be able to browse for available user names (Possibly OBE by design)

JEDI 2.0 Requirements

- **Floating Configurable Security Classification Banner**
  - Banner shall interoperate with Clear Temp
  - Banner shall remain "on top" of any window
  - Displayed at top or bottom
    The banner shall go completely across the screen
  - User shall not be able to close this banner
  - Display classification on screen saver

- **Support for Windows Server 2003, 2000,XP**
  - JEDI shall run on Windows Server 2003,2000,XP systems
    - The software shall run on a minimum of the Standard, Enterprise Editions Server, Advanced Server and Professional of the software
  - Take advantage of RunAs Service
  - Remove SU service

JEDI 2.0 Requirements

- **2003,2000 Server with mixed clients**
  - JEDI shall support Windows 2000 and XP clients, with a Windows 2003,2000 server
  - Support Terminal Services
  - Support Smart Cards
  - Installation using WISE Installer
  - JEDI shall provide documentation on how install using RIS. JEDI shall provide documentation on how to set up a RIS Server for Windows 2003
  - Installation shall be MSI compatible
  - Upgrade AFDI 1.2 to JEDI 2.0 and Windows 2000 to 2003 Servers.
  - Preserve configuration
    The JEDI upgrade shall preserve the AFDI 1.2 configuration and re-configure JEDI 2.0 with the identical configuration
  - JEDI shall provide documentation to upgrade Windows 2000 networks to Windows 2003. Make use of existing white papers from Microsoft that detail this procedure

JEDI 2.0 Requirements

  - CAB file
    The CAB file shall be updated to support this release for the JAVA console
  - Windows 2003,2000,XP supported editions
    The software shall run on a minimum of the Standard and Enterprise Editions for 2003 and Server and Advanced Server on 2000 and Professional for XP

- **Configure JEDI tools for Windows via MMC Plug-Ins**
  - JEDI shall use the Microsoft Management Console (MMC) plug-in functionality. All user configurations of the JEDI tool set shall be done through a MMC plug-in
- **Device Lock**
  - Create and remove device groups.
    The user shall be able to create groups (cdrom, floppy, jaz, tape, USB and zip) for the device lock utility
  - Lock users from a device
    The user shall be able to assign and unassign users to the device group. The user shall be able to view the currently assigned users in a device group

JEDI 2.0 Requirements

  - Device Lock shall periodically check for removable devices. If a new device is found then it shall be locked (OBE by COTS Devicelock)
  - Set permissions on devices
    The users shall be able to create hard links for each device to allow read, write and/or executable permissions

- **Password Filter**
  - JEDI shall create an MMC plug-in to configure the password filter functionality
  - Move Password settings into Registry
- **Security Banner**
  - JEDI shall create an MMC plug-in to configure the security banner functionality
  - Put Security Banner settings into Registry
  - Create a standard set of Classifications

JEDI 2.0 Requirements

  - Allow selection of Colors for Foreground and Background The default colors shall be yellow background and black text

- **Screen Lock and Deadman**
  - JEDI shall create an MMC plug-in to configure the screen saver and deadman functionality
  - Move Screen Lock settings into Registry
- **Login Consent Banner**
  - JEDI shall support Smart Card and other biometric devices Smart Card insertion shall not automatically select agreement to Logon Consent
  - JEDI shall create an MMC plug-in to configure the login consent functionality
  - Text Color and font shall be configurable
  - The default colors shall be yellow background and black foreground

JEDI 2.0 Requirements

- **Accept/Decline action**
  - The banner shall write an audit containing the username and action taken
  - The banner shall timeout if no action is taken (configurable)
  - The banner shall be able to allow both keyboard and mouse support
  - The banner shall support pressing the spacebar or the return key for acceptance of the message
- **Clear Temp**
  - JEDI shall provide the ability for a privileged user to configure the directory(s) that will be cleared in Clear Temp. Directories shall be selectable, using system variables and user variables
  - JEDI shall create an MMC plug-in to configure the Clear Temp functionality
  - Clear Temp shall run when the user logs off. Clear Temp shall be configurable to run at login

JEDI 2.0 Requirements

- **System Help**
  - The system shall include on-line help
- **Release Notes format on CD**
  - The release notes shall be readable in notepad and on installation page
- **AFDI Uninstall process not as expected**
  - The uninstallation of JEDI shall be automatic by not requiring the user to acknowledge locked or shared files
- **CLASS GUI disappears with Windows 2000**
  - The windows CLASS utility shall not cause the Solaris CLASS server to disappear
- **Deadman Blue Screen**
  - JEDI shall correct the memory leaks in the deadman utility
- **Remove LANguard**
  - LANguard shall be removed from the JEDI 2.0 software

JEDI 2.0 Requirements

- **ISS**
  - JEDI 2.0 for Windows shall include the Internet Security Scanner. ISS shall be included with the JEDI distribution but will not be included in the JEDI installation. A basic installation shall be documented and the ISS documentation shall be referenced. The security risks shall be documented in the SSAA; the security templates for ISS shall be documented in the Known Risks and Vulnerabilities section of the SSAA
- **FSD Management on Windows**
  - JEDI 2.0 shall add a tab to the User Manager to add Full Services Directory data. The schema for the Active directory shall be modified to add the FSD fields and the FSD data shall be placed therein
- **Referenced Documents**
  - All documentation shall reference current documentation

Questions

Questions???

Design Overview

- JEDI 2.0 will run on Windows 2003/XP/2000 versions
- Move to an .msi installation package
- Move configuration settings to the registry
- Make sure configuration settings can be modified through the Microsoft Management Console(MMC) using the JEDI Management Console (JMC)
- Improve all utilities but especially Event Backup and Print Utility

Installation

Purpose

The JEDI 2.0 Windows Installer will install the JEDI software and provide users with an interface to completely configure an operational JEDI workstation. This design will initially detail the enhancements proposed for the JEDI 2.0 Windows Installer.

Current Functionality

The current AFDI Windows Installer was written as a self contained InstallShield application for Windows 2000. It provided the following functionality:

- Display an HTML splash page upon insertion of the CD-ROM
- Verify correct Operating System and Service Pack version
- Check for administrative privileges
- Display Release Notes
- Install in any directory
- Installation types of Typical, Complete, and Custom
- Ability to select individual components
- An interface to configure ISD, CLASS, Print Utility, Event Backup, Watchdog, Deadman, NTP etc.
- Apply NSA security template

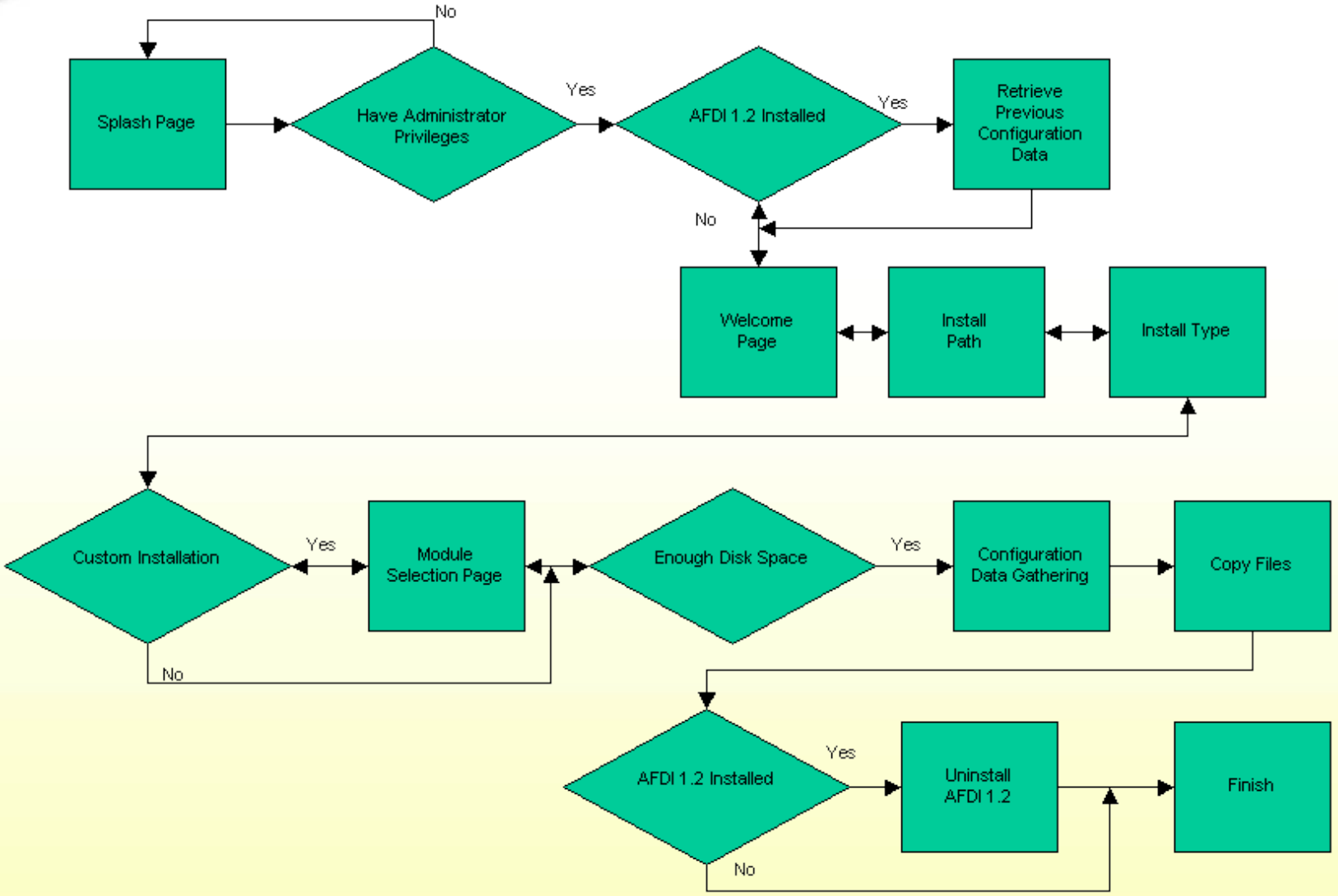
Installation

Proposed Functionality

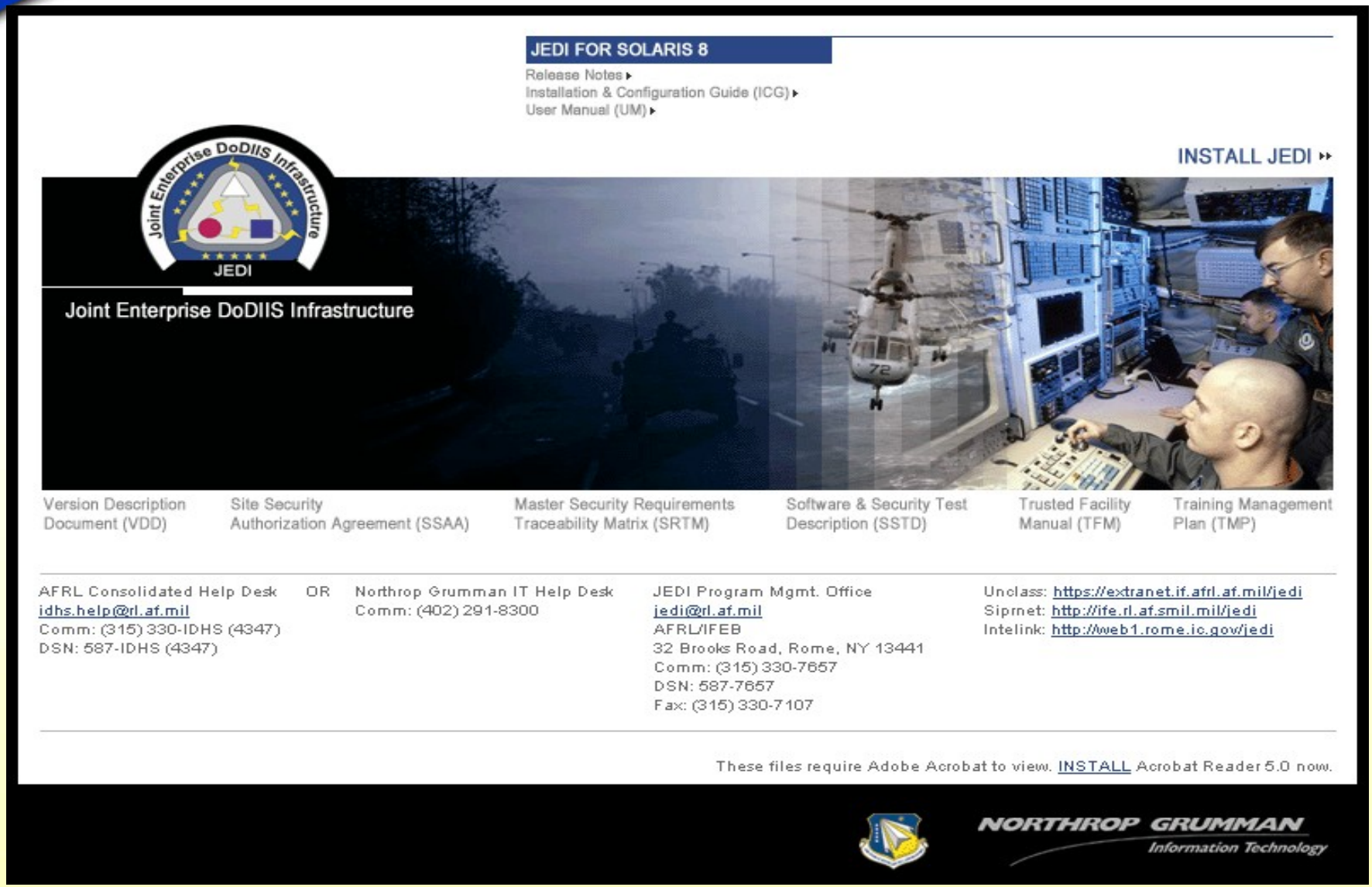
The proposed JEDI 2.0 Windows Installer will maintain the previous functionality. Several enhancements will be made to improve and augment the current functionality.

- The installation program will be written using the Wise Installer for Visual Studio .NET
- Installer will be completely MSI compliant to support rapid deployment (RIS)
- Support for Windows 2000/XP/2003
- Add new utilities to installation package
- Add configuration panel for system classification
- Remove deprecated utilities (NTP, LANguard, SU Service)
- Correctly display available and required disk space
- Provide option to use JEDI, DIA, or custom security templates
- Provide ability to run the “Security Analysis and Configuration” MMC snap-in after installation
- Provide ability to run “JEDI Management Console” MMC snap-in after installation
- Better installation and configuration of Event Backup and Print Utility
- User configuration will occur before files are copied into place

Installation Processing Diagram



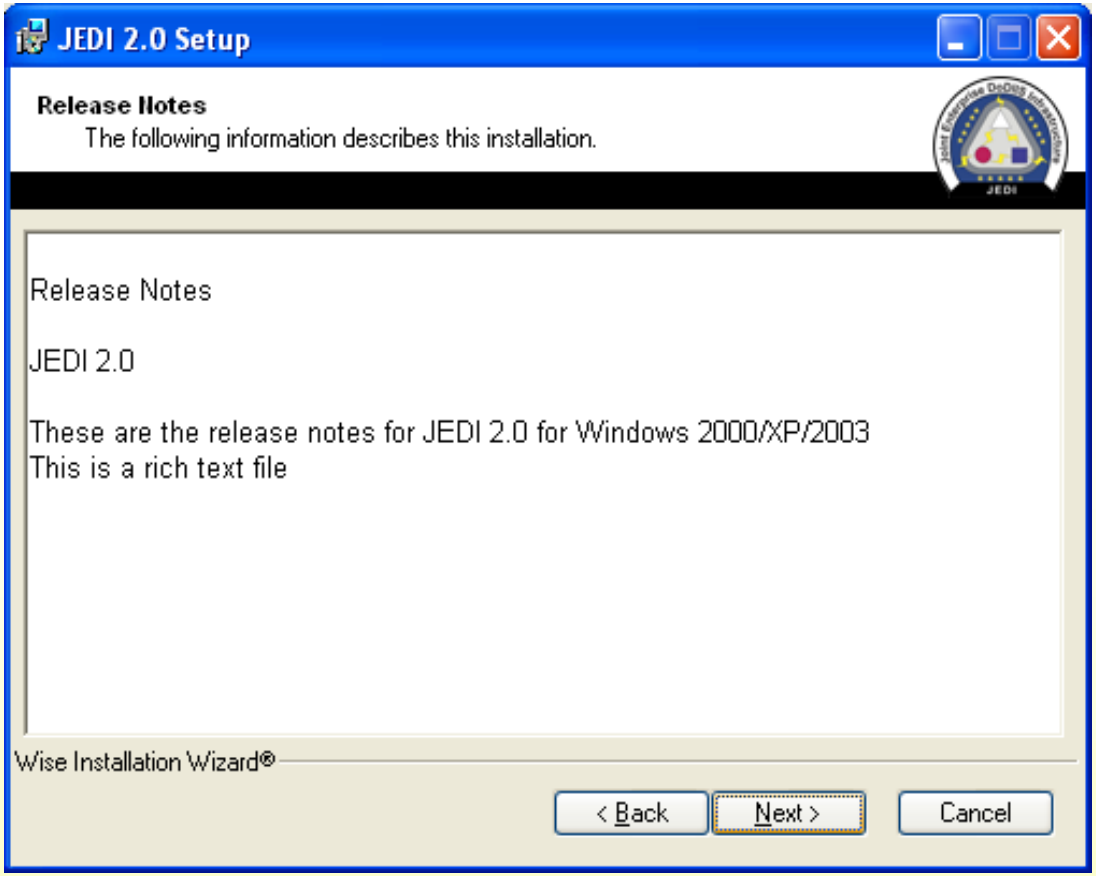
Installation Autorun Screen



Welcome Page

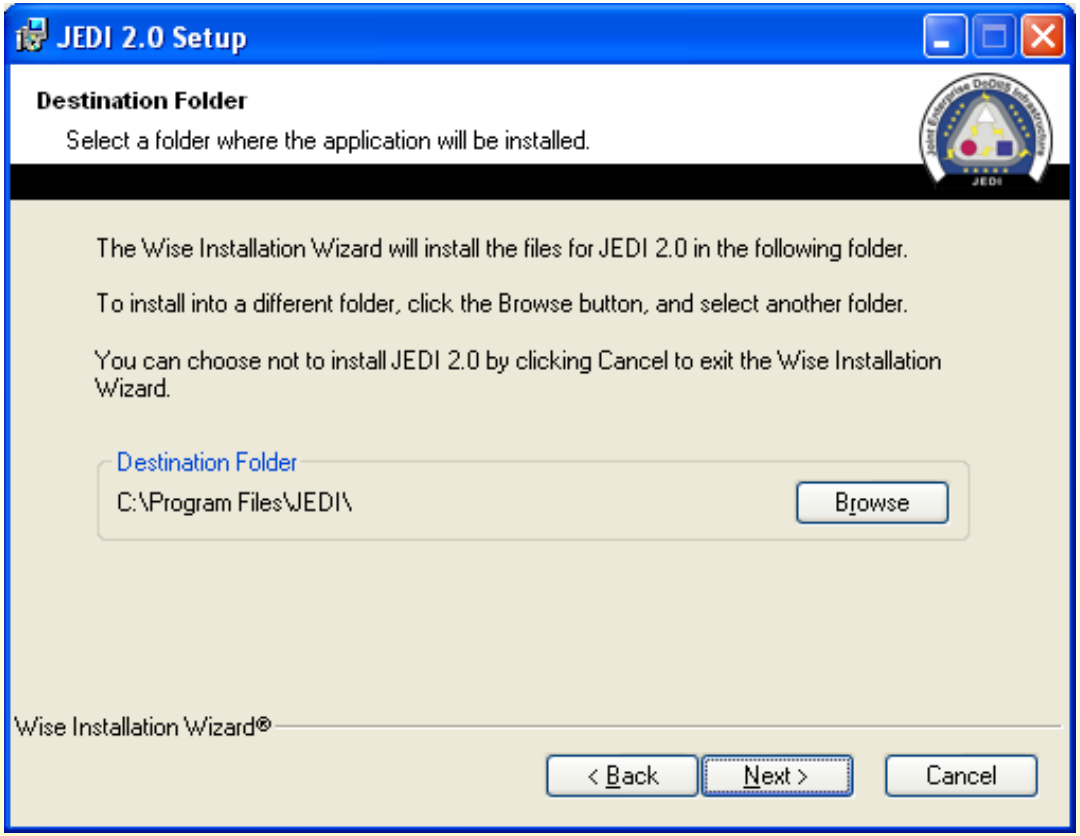
- Checks will be made to ensure the user has correct privileges and the Operating System and Service Pack versions are correct

Release Notes



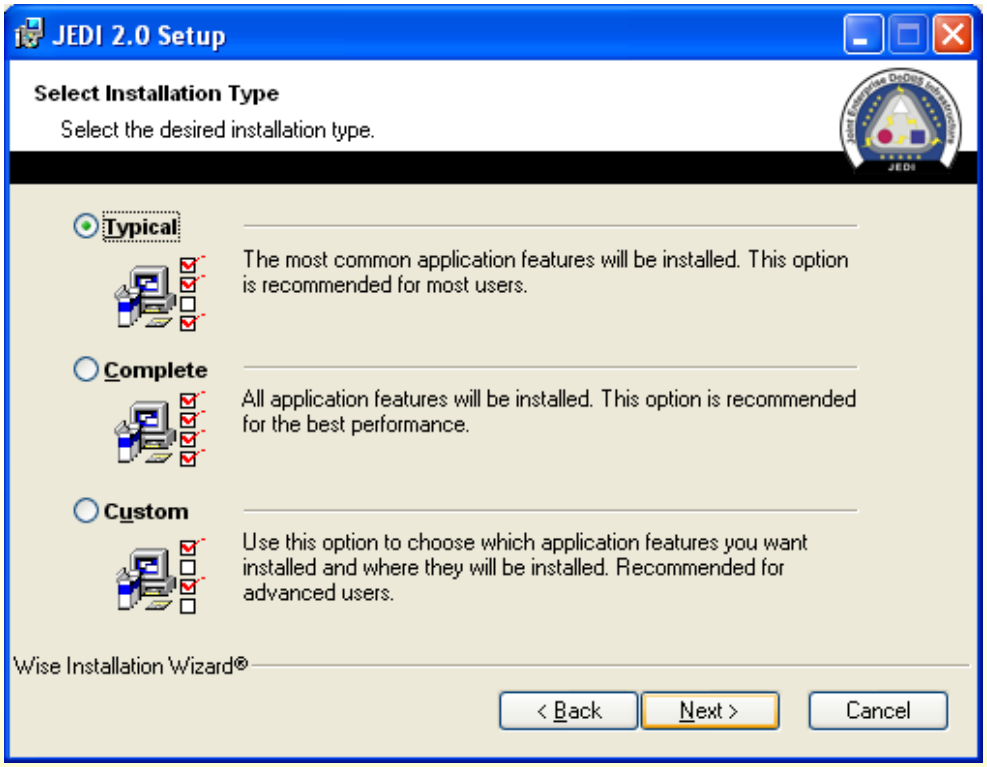
- Simple installation window displaying the release notes
- Release Notes are the same as the one placed onto the CD-ROM

Destination Folder



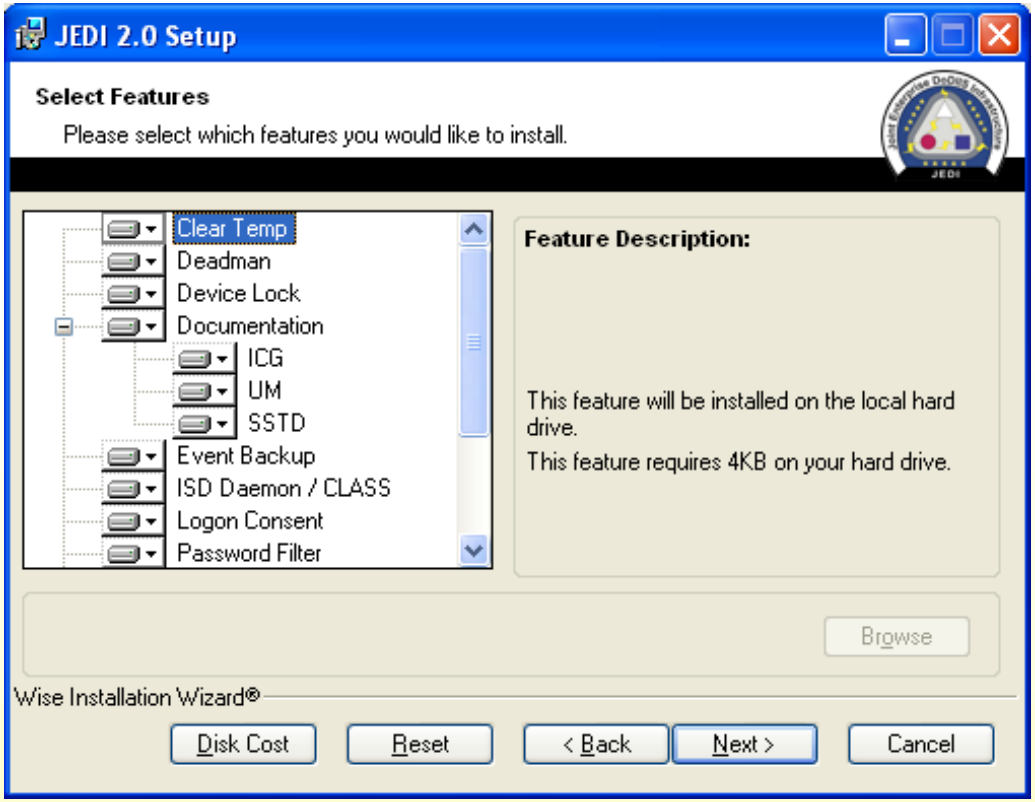
- This installation window allows the user to select the location to install JEDI
- The “JEDI” directory will be created automatically unless already specified in the path chosen

Installation Type



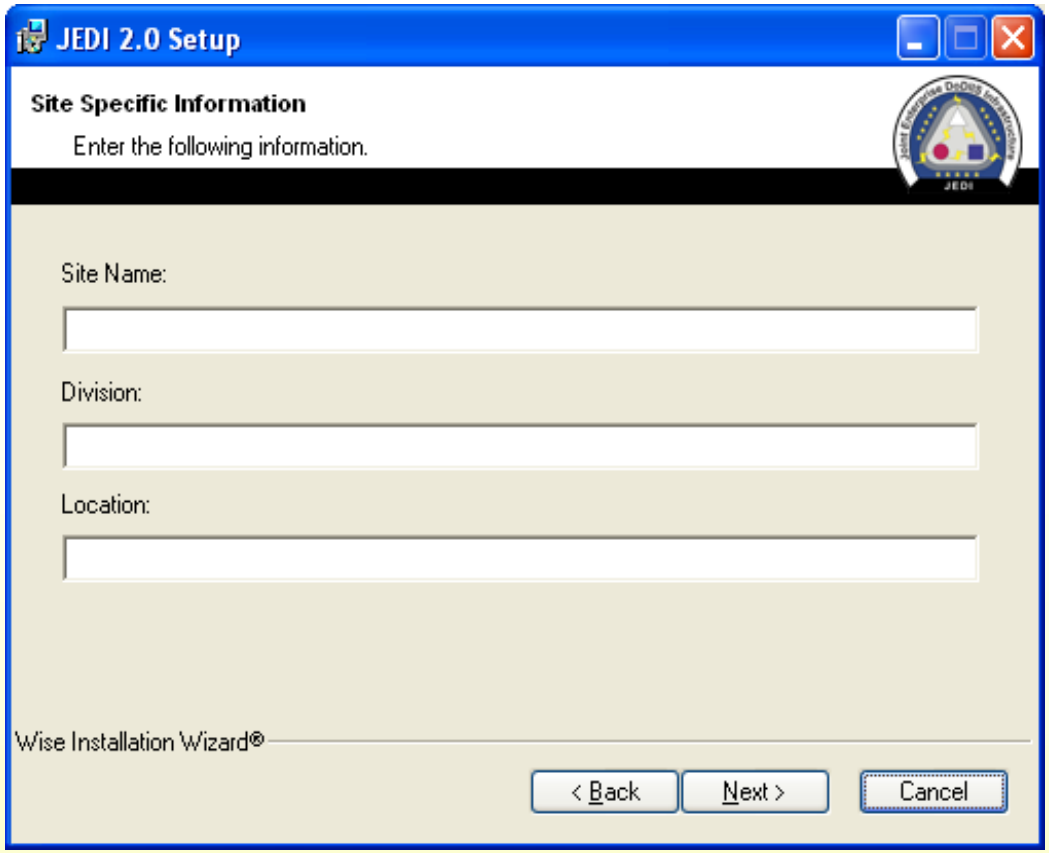
- The user shall be provided the option to choose one of three installation choices: Typical, Full, and Custom
- **Typical**: install all components except ISD, CLASS, and the PDF and Word formatted documentation
- **Complete**: will install everything
- **Custom**: will allow the user to select which modules to install

Select Features (Custom Install)



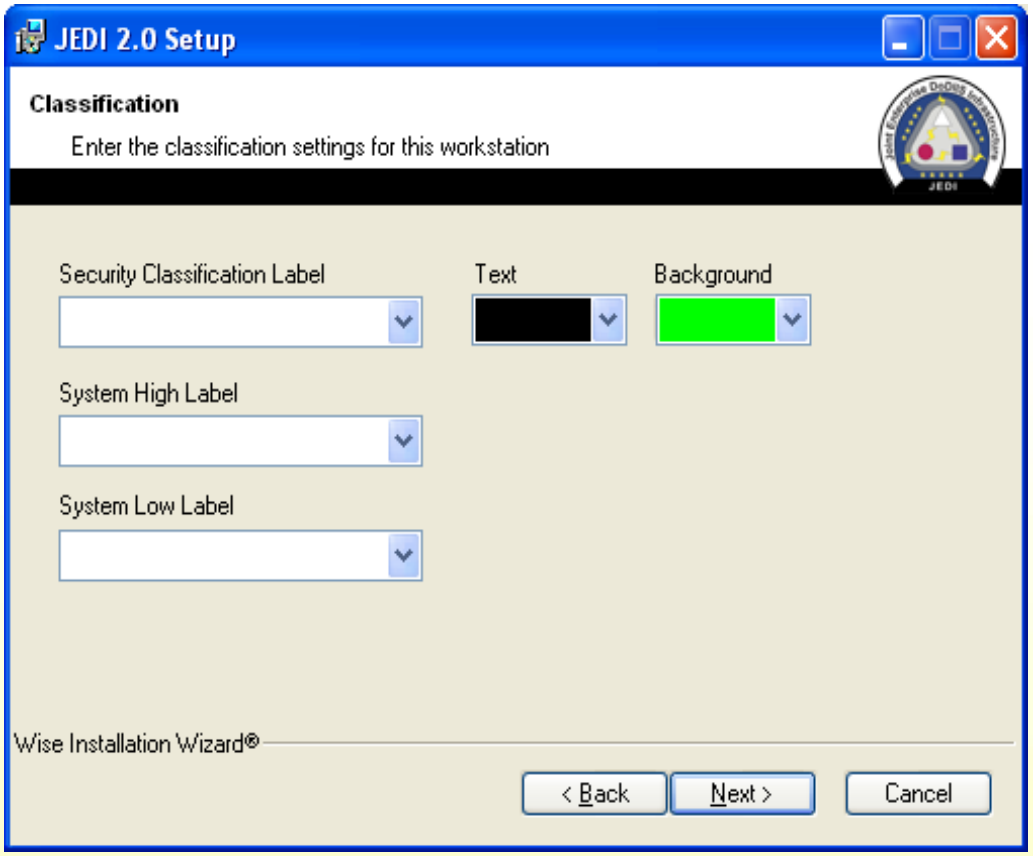
- If the user selects custom install, they will be provided a list of components to install
- Highlighting each item will give a small description of that module
- All modules can be installed on any type of workstation
- A “core” module will always be selected which contains the required files for all JEDI installations

Site Specific Information



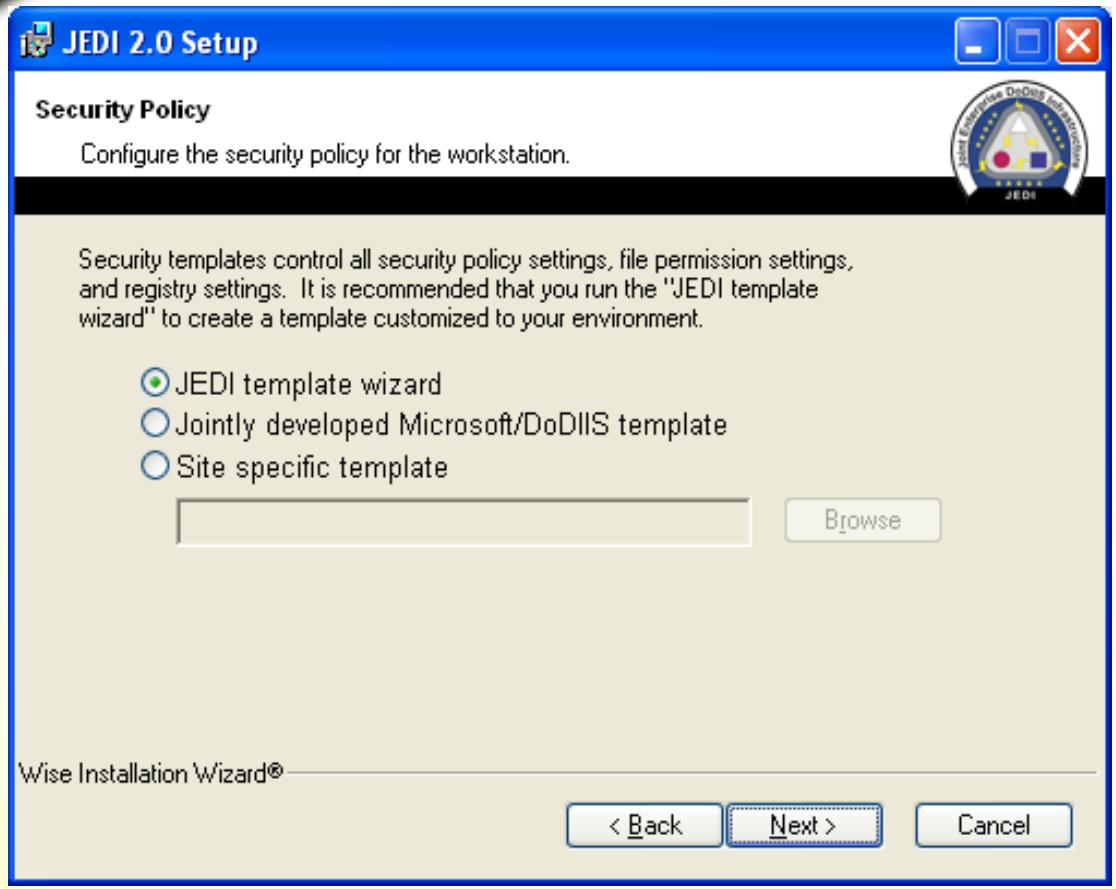
- The user can enter any Site Specific Information

Classification



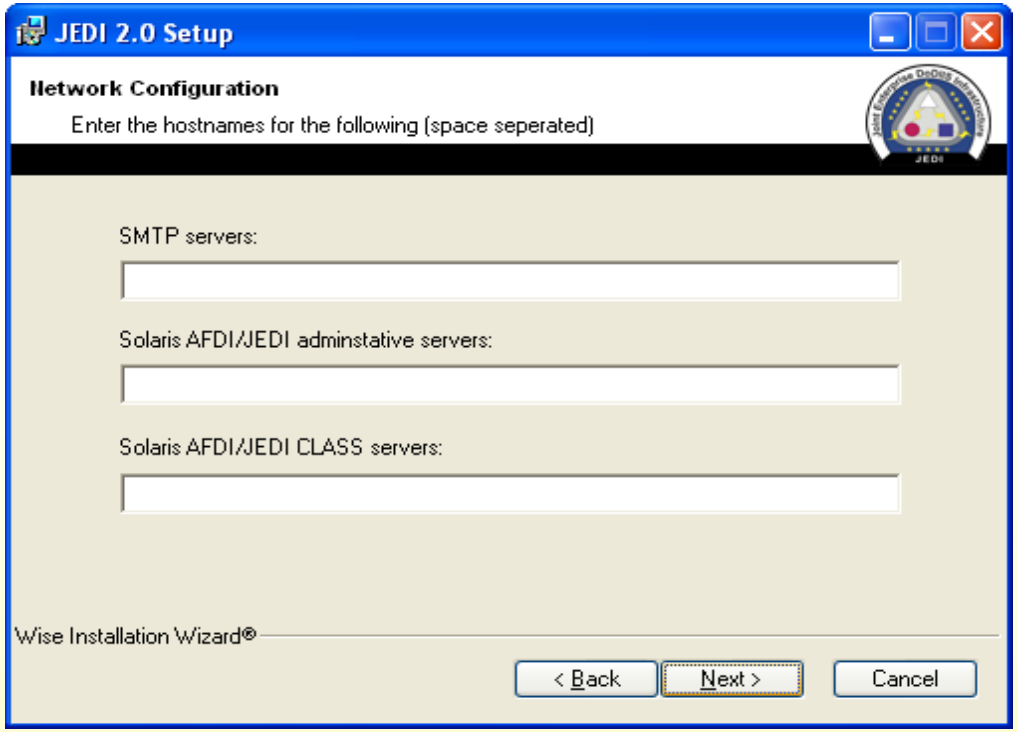
- The user will be given the option to set the Security High and Security Low classifications for the workstation
- This will implement a global policy for the system. Unclassified, Secret, and TS-SCI will be included by default
- The user will also be given a choice to select a custom classification label and color scheme

Security Policy



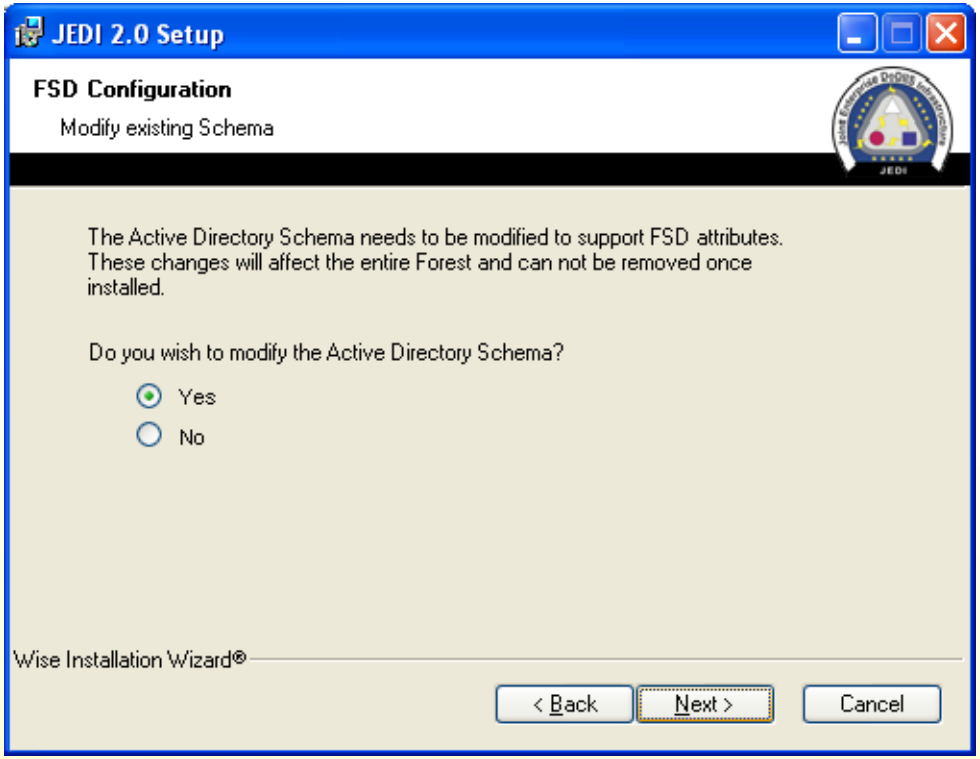
- Users shall be provided the option to apply either our custom security template or their own custom security template
- These templates are applied outside the scope of the installer and cannot be rolled back to the systems previous settings once applied
- The user will also be presented with an option to apply these settings either automatically or

Network Configuration



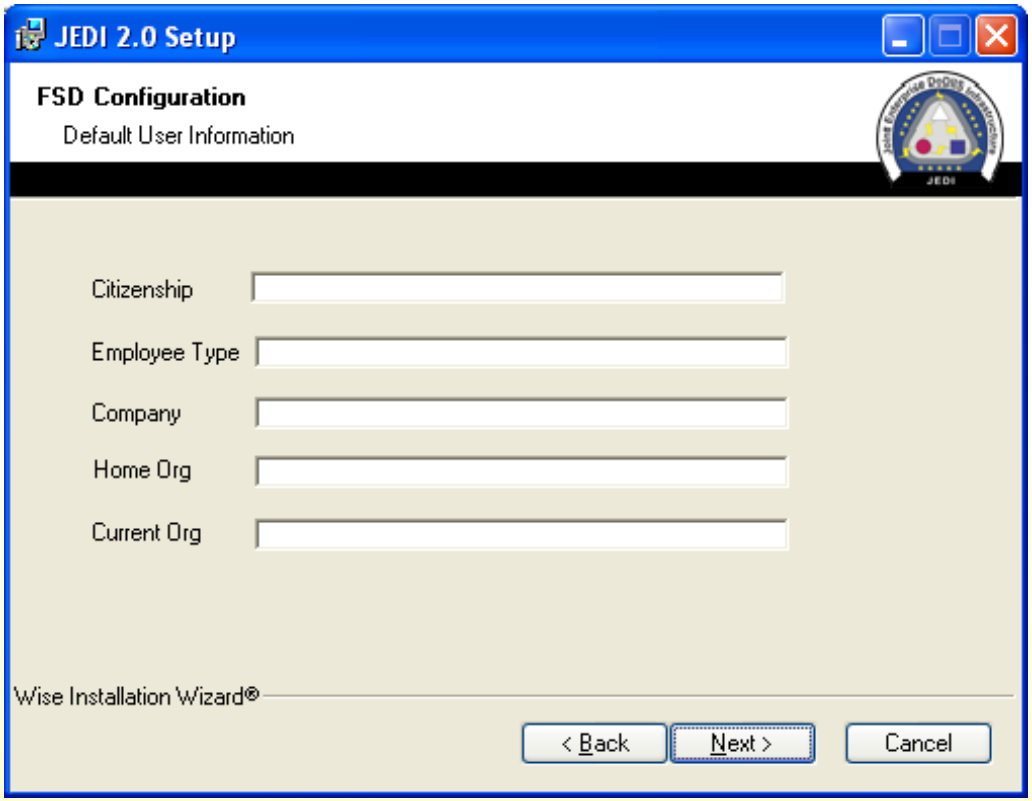
- To provide UNIX interoperability the user must specify the hostnames of their JEDI Administrative workstations, JEDI CLASS Servers, and SMTP server

FSD Schema Modification



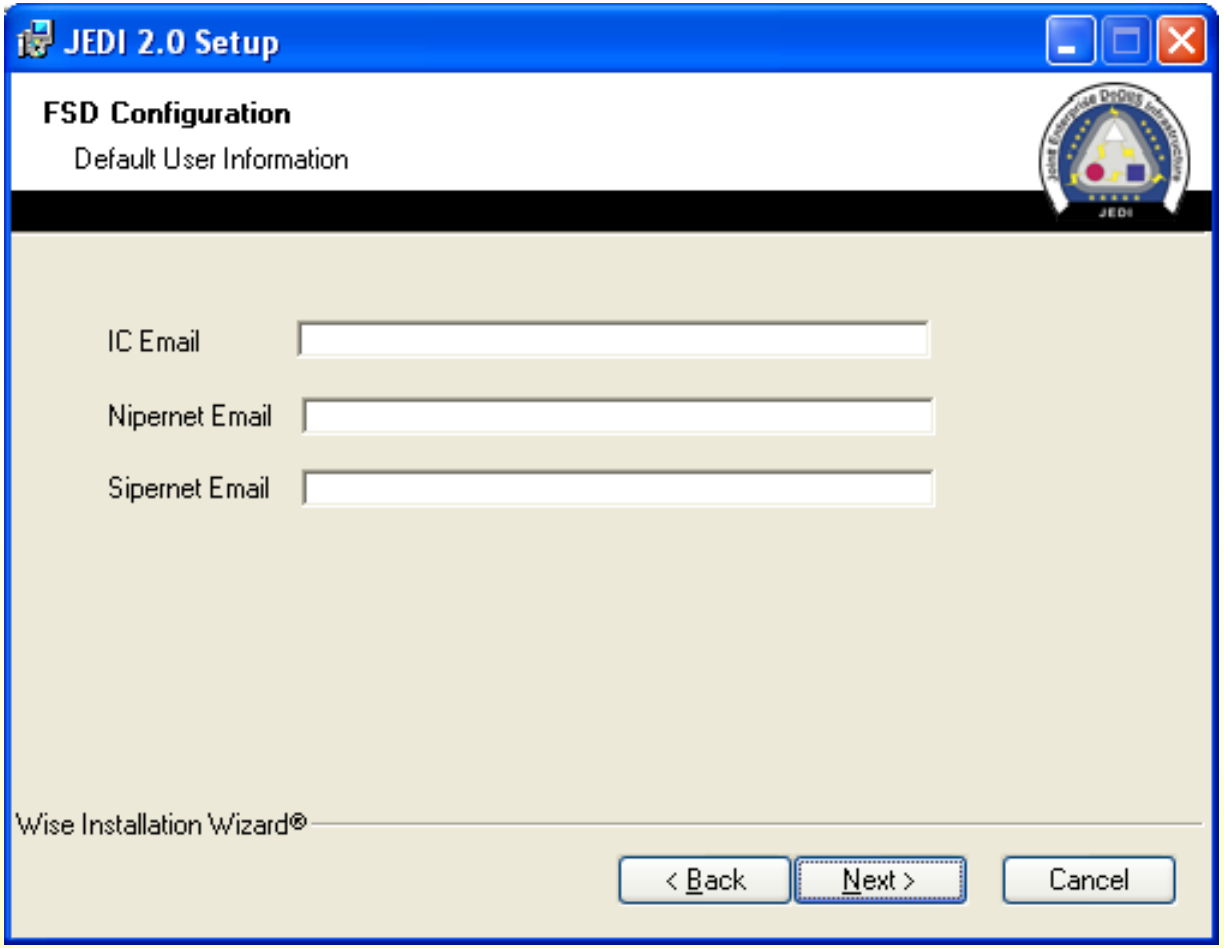
- Give the installer the option to install the FSD Schema changes and utility

FSD Defaults



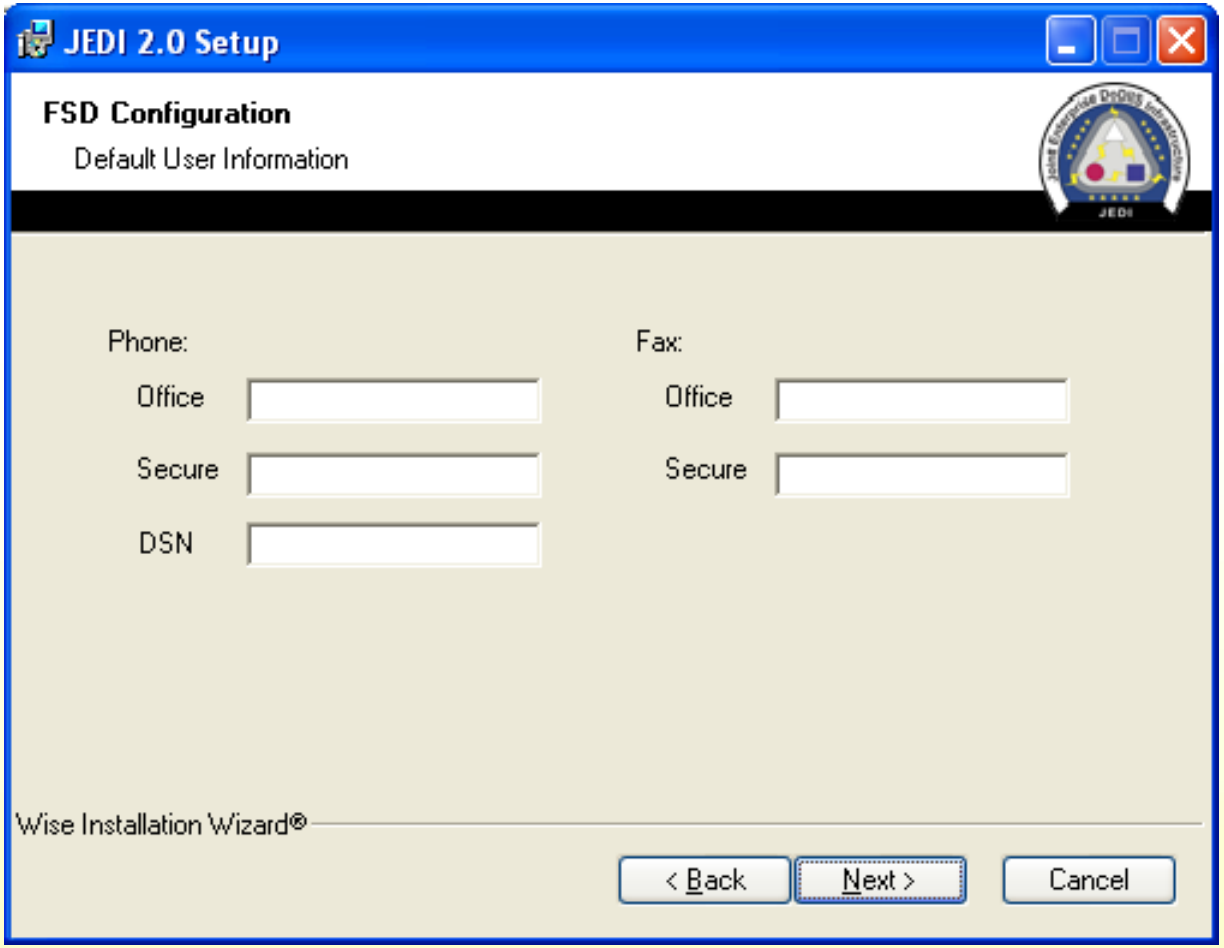
- The following screens are used to gather default data for FSD fields

FSD Defaults



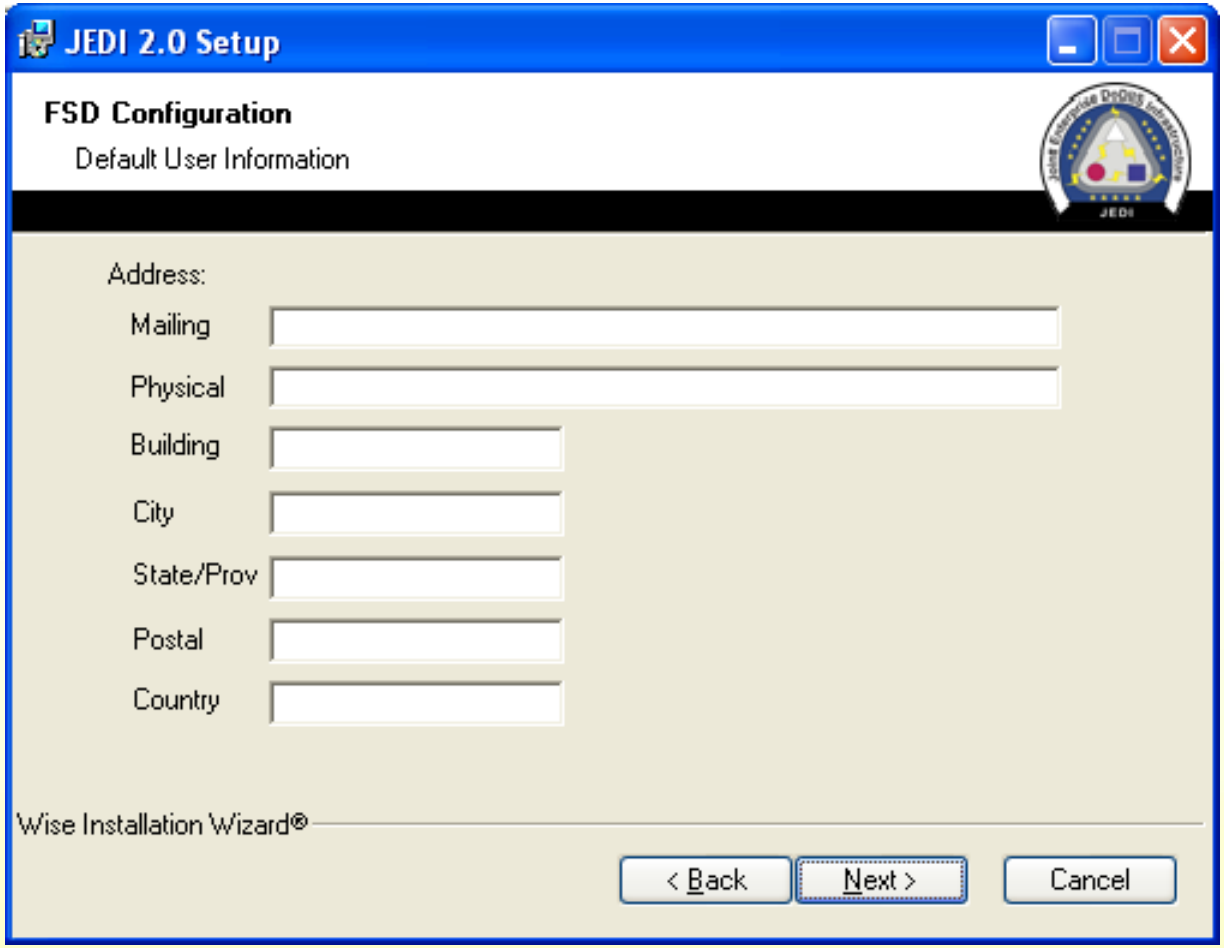
- Configure Mail for FSD

FSD Defaults



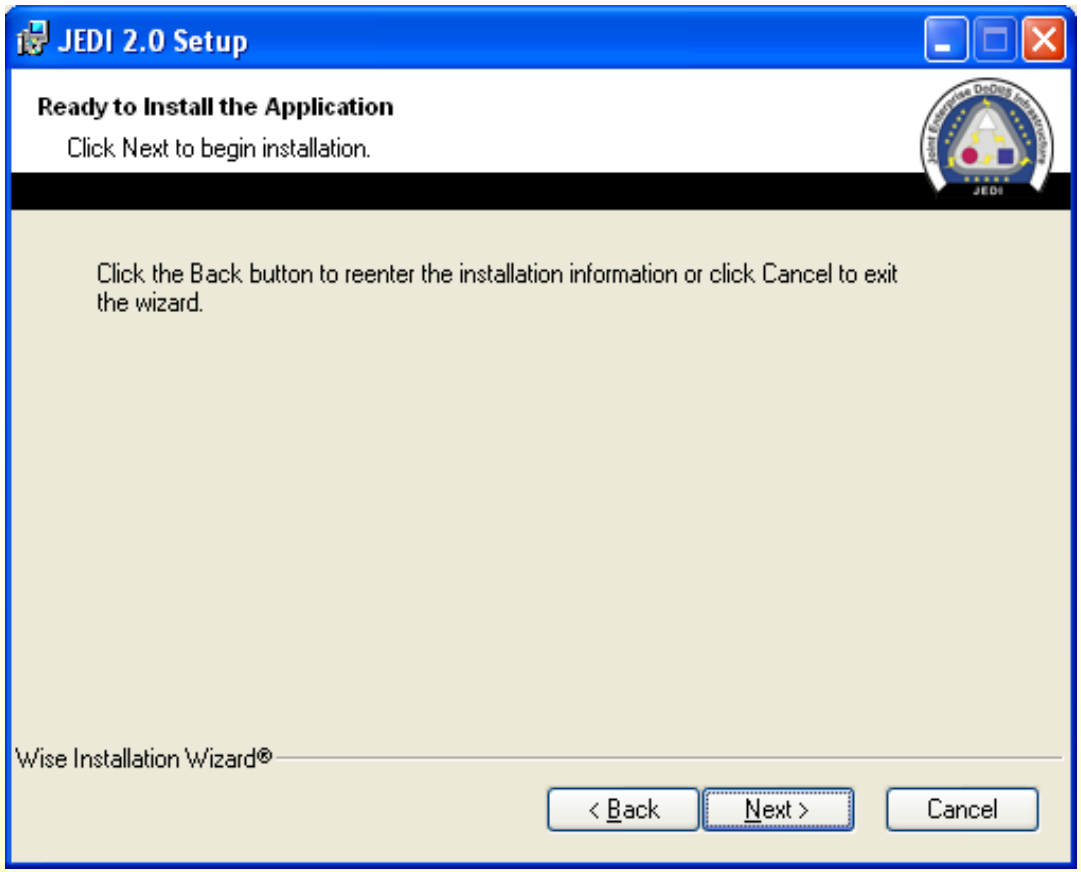
- Configure Phone and Fax for FSD

FSD Defaults



- Configure Address for FSD

Setup Finish Screens



- Files and registry settings will be installed

Setup Finish Screens

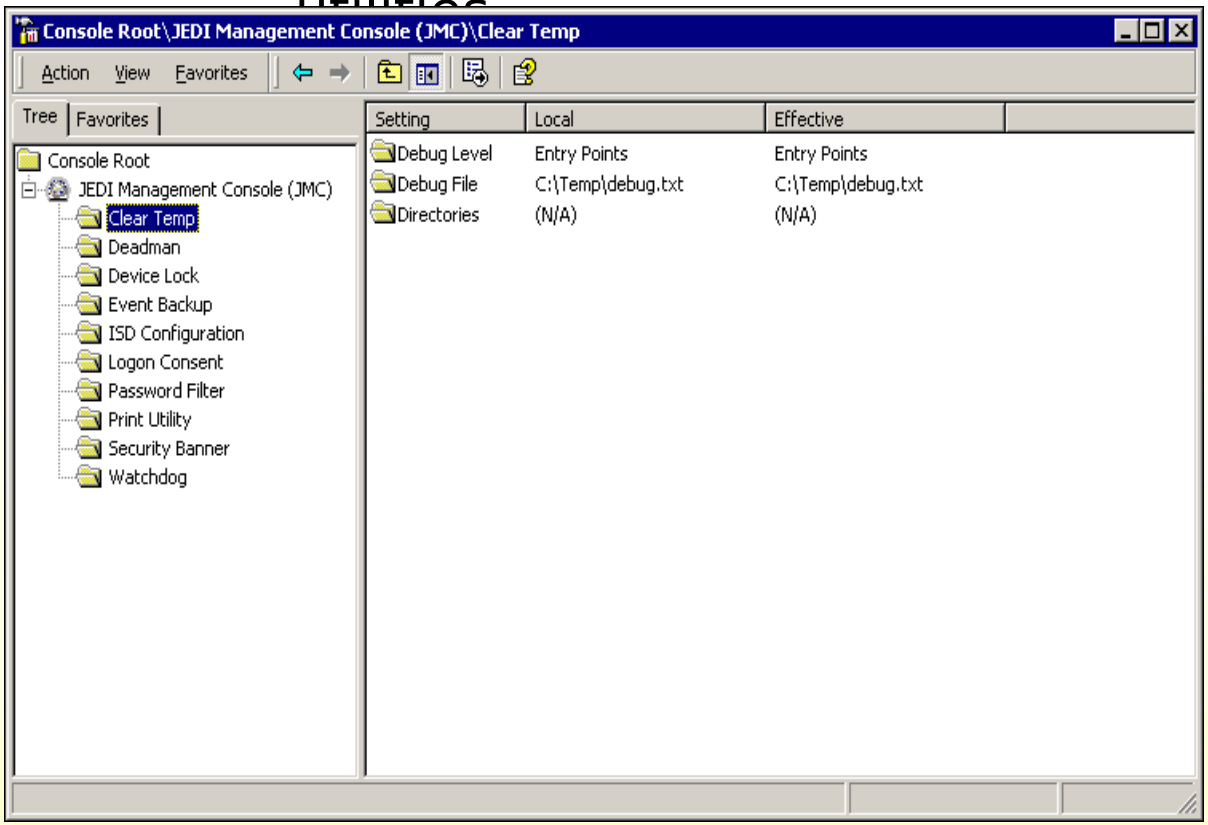
- A reboot may only be needed after an upgrade

Questions

Questions???

JEDI Management Console

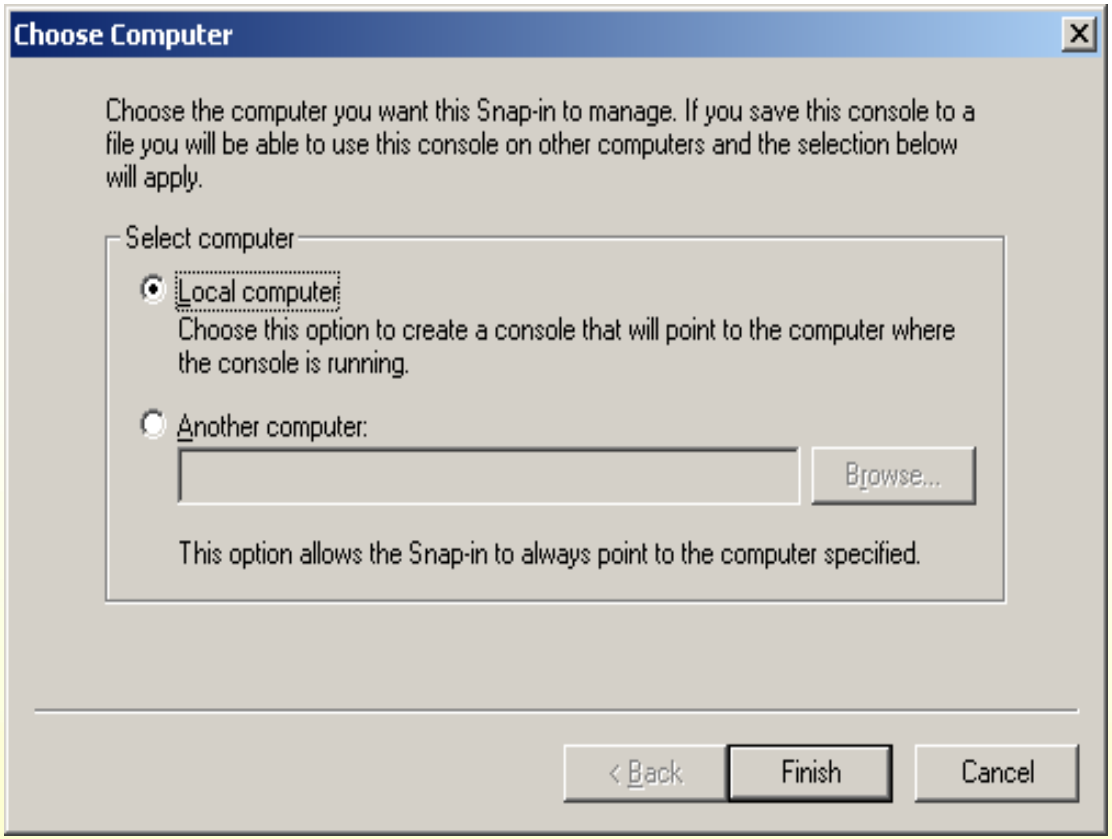
The JEDI Management Console (JMC) is an MMC snap-in to configure the various JEDI utilities



- Select utility in the Left tree view
- Settings will be displayed in the main window
- Local setting and Effective settings are displayed

- Double clicking on any entry will bring forth the corresponding configuration GUI for that setting

JEDI Management Console



- MMC will allow the configuration of the local settings on remote hosts

Password Filter

Purpose

The Password Filter provides a mechanism to do checks on password when a user changes their password.

Current Functionality

The JEDI 1.2 Windows Password Filter utility currently utilizes an enpasflt.ini file to store the configuration settings for the utility.

When installed, the following default password rules are in place:

- The password must contain at least eight characters *
- The password must contain at least one upper case character *
- The password must contain at least one numeric character *
- The password must contain at least one special character *
- The password cannot contain the user's account name, or the reverse spelling of the account name

Password Filter

Current Functionality (cont.)

- The password cannot be a dictionary word, or a dictionary word with leading or ending special and/or numeric characters
- The password cannot contain more than the specified number of consecutive repeating characters (default is two repeating characters) *

Note: Configurable password rules found in the ini file are indicated by an asterisk (*)

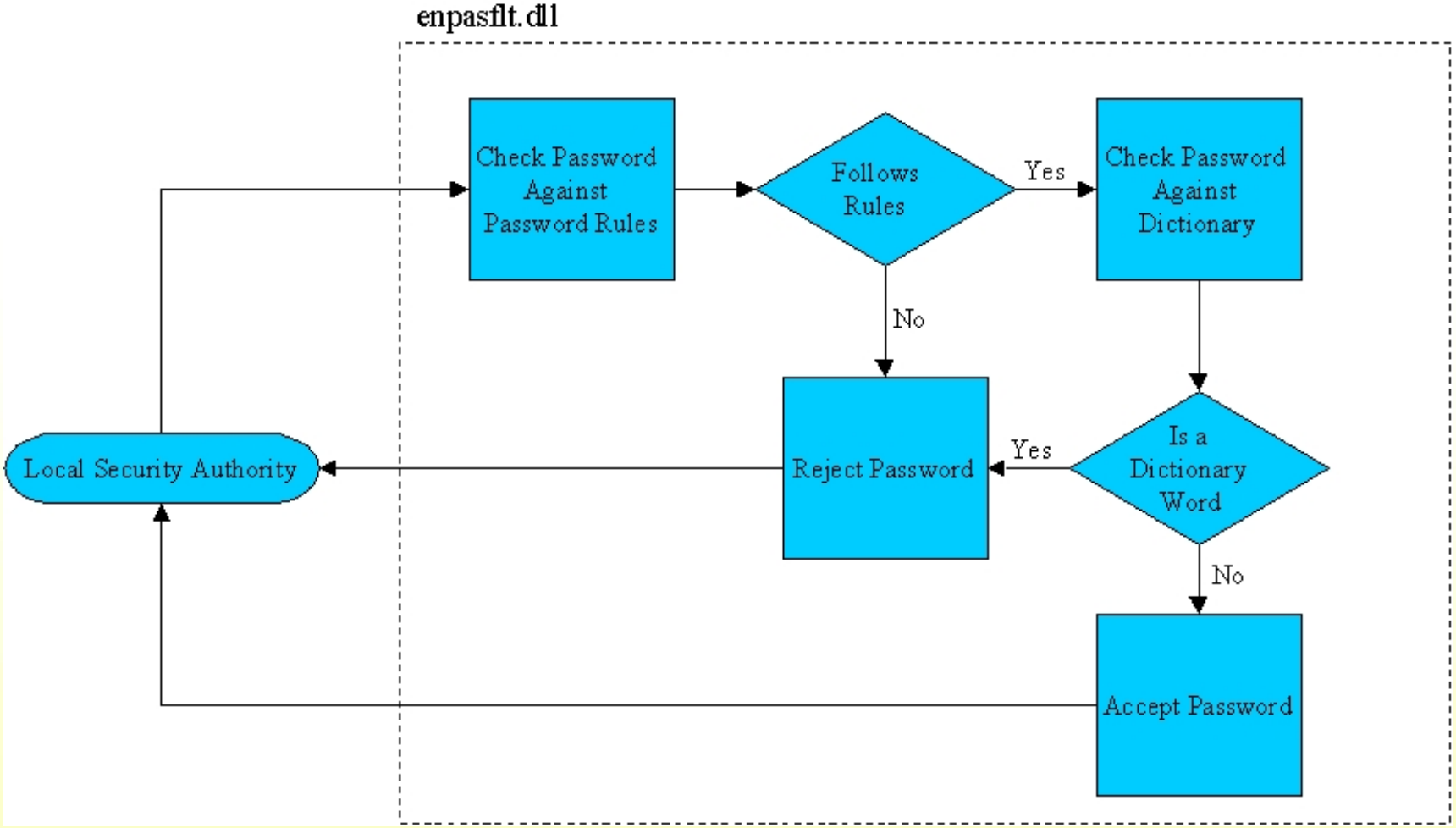
Password Filter

Proposed Functionality

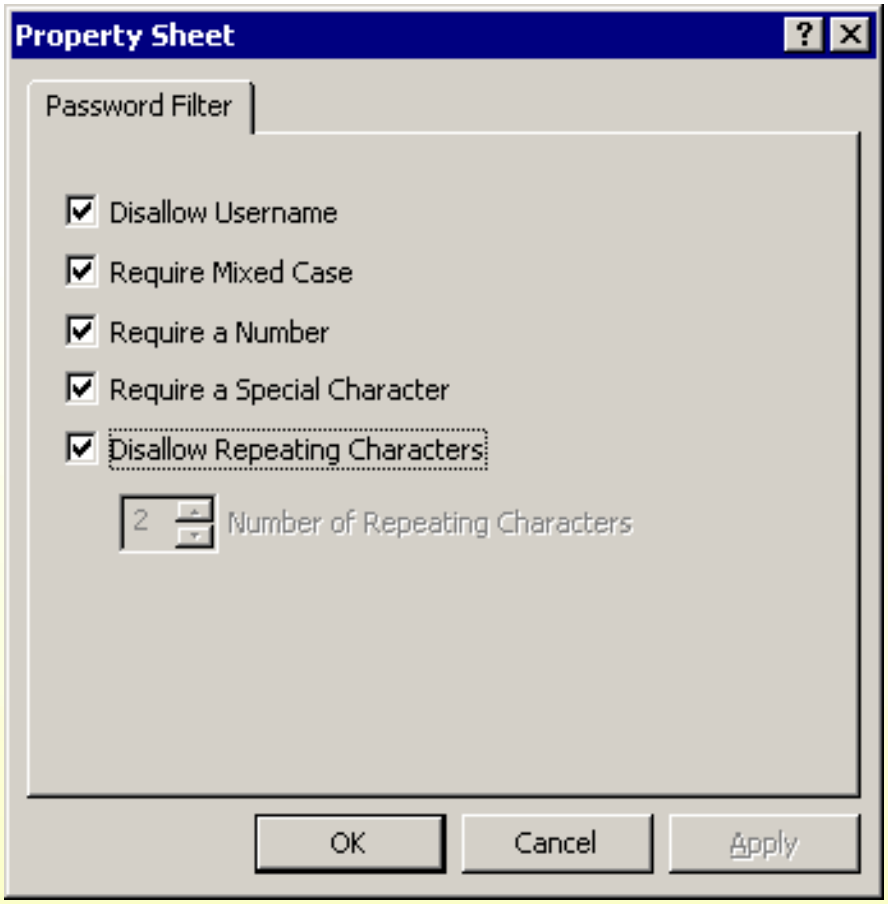
The password rules will remain the same, and configurable rules identified above will remain configurable. The following list contains the proposed changes.

- Modify the JEDI Windows installation program to place the configurable password rules in the Windows Registry in place of the enpasflt.ini file
- Modify the Password Filter utility to access the configurable password rules from the Windows Registry instead of from their current location in the enpasflt.ini file
- Create an MMC plug-in GUI for configuration of those password rules stored in the Windows Registry

Password Filter Processing Diagram



Password Filter



- This panel allows for the configuration of the rules to be applied to the passwords when they are validated
- This panel is called from the JMC console

Questions

Questions???

ISD

Purpose

The Infrastructure Services Daemon (ISD) assists sites at integrating Windows networks with UNIX networks. This design will initially detail the proposed enhancements for the ISD.

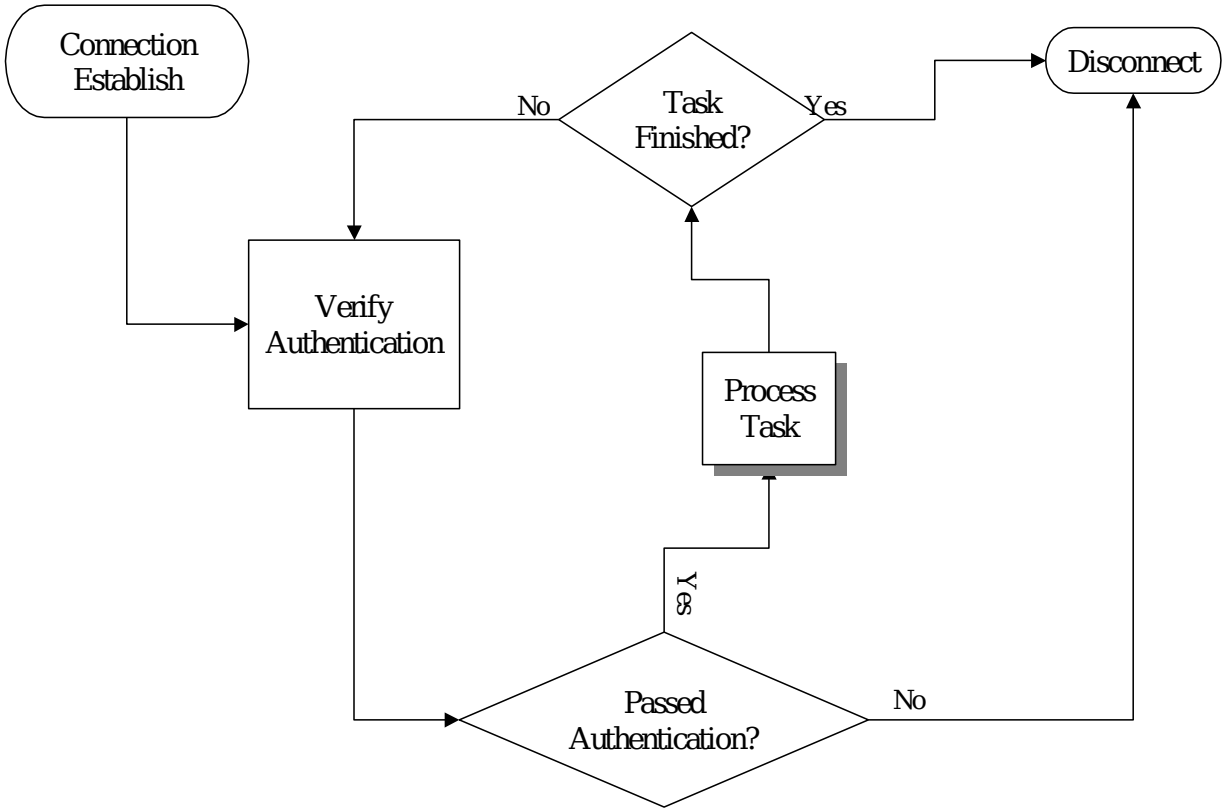
Current Functionality

- Executes at startup as a service
- During the service startup, the ISD reads the file isd.ini. This file is similar to the isd.conf file found on the JEDI UNIX release
- Provides hostname, UID, and GID security for the following utilities:
  - Disk Space
  - Process Management
  - User Account Information
  - User Account Maintenance
  - Boot Utility

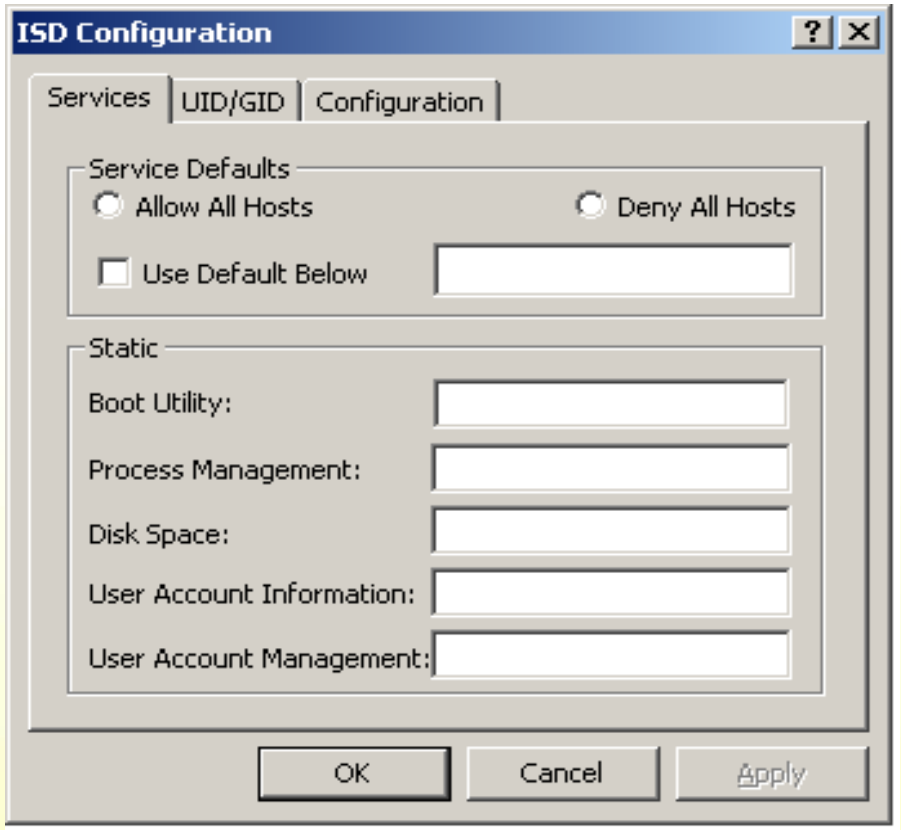
Proposed Functionality

- Move isd.ini into registry
- Configurable from a MMC GUI
- Must support Terminal servers (Remote Desktop)

ISD Processing Diagram

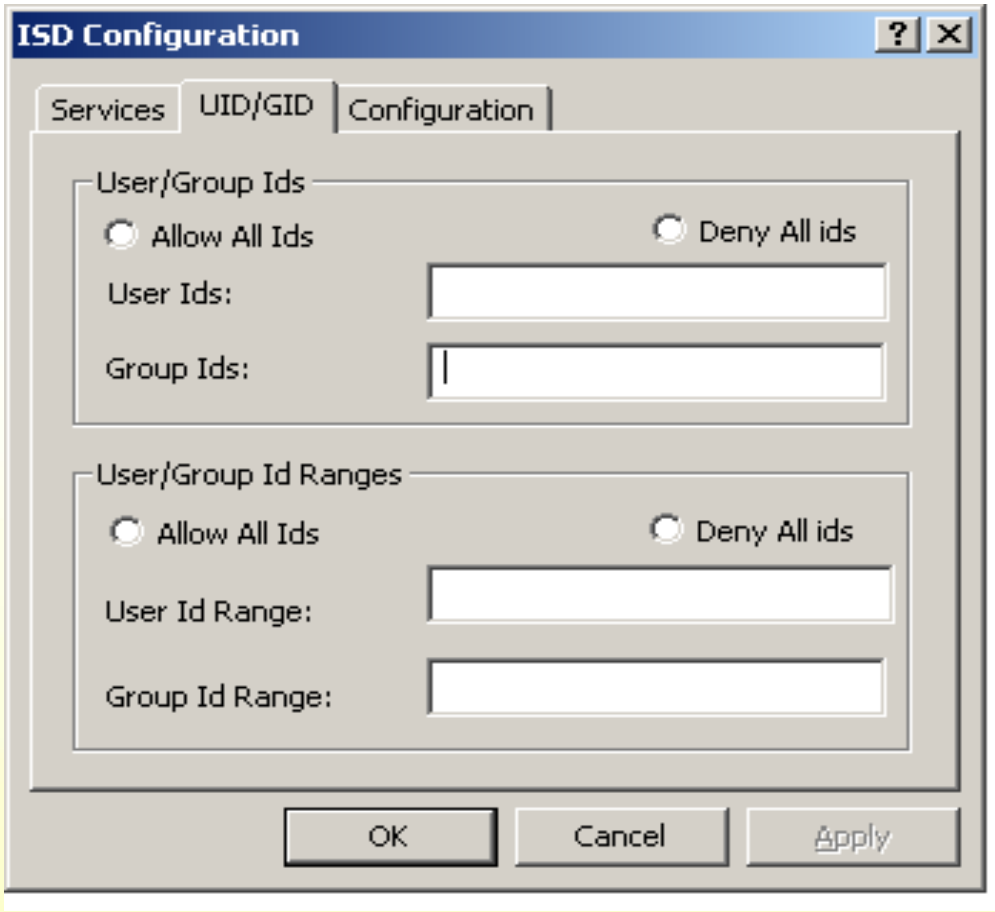


ISD



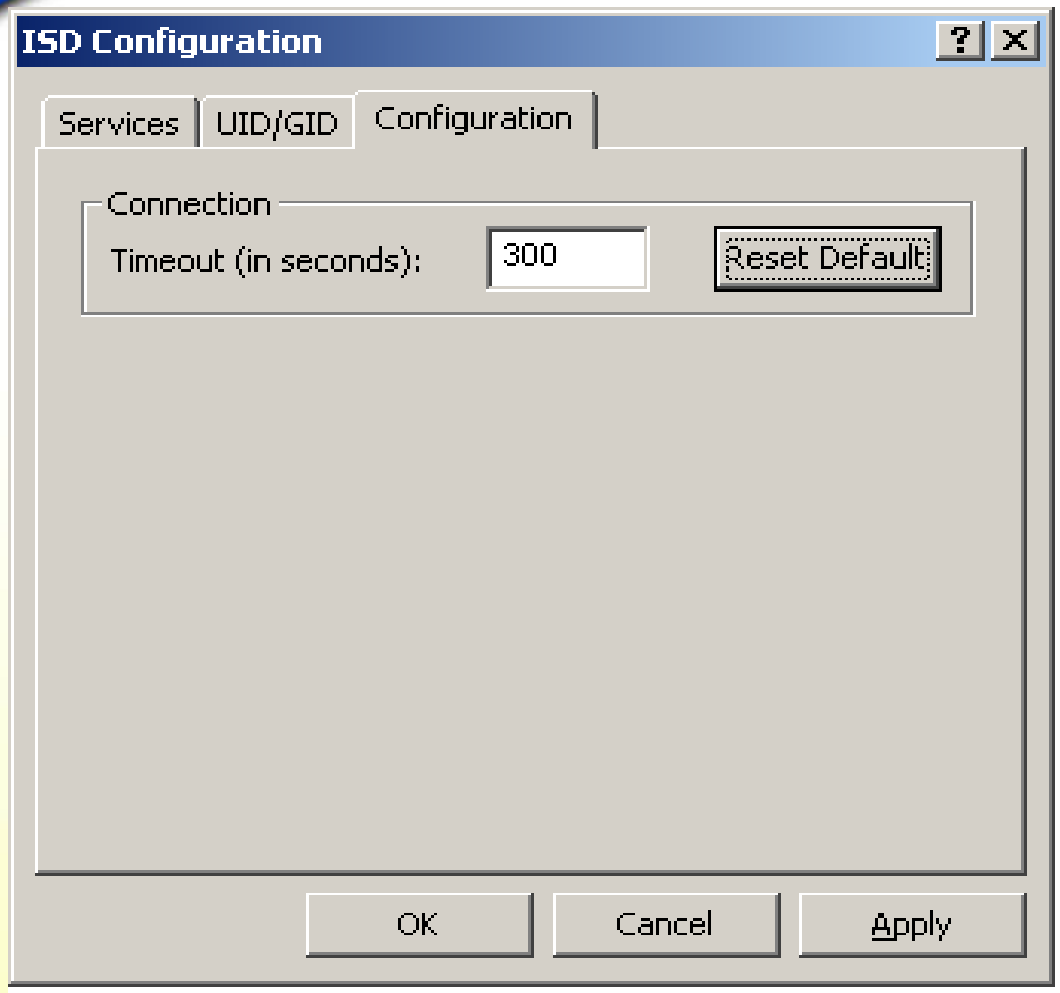
- Allows only the entered Hostnames access to the ISD functionality or Denies all Hosts
- This panel is called from the JMC console

ISD



- Enter UNIX User and/or Group Ids
- Enter UNIX User and/or Group ranges
- This panel is called from the JMC console

ISD



- Configuration Tab to disconnect stale connections after 300 seconds

Questions

Questions???

Watchdog

Purpose

Watchdog will be modified to use existing Windows functionality to restart a failed service. In its diminished role, Watchdog will send email notification of service failures when they occur.

Current Functionality

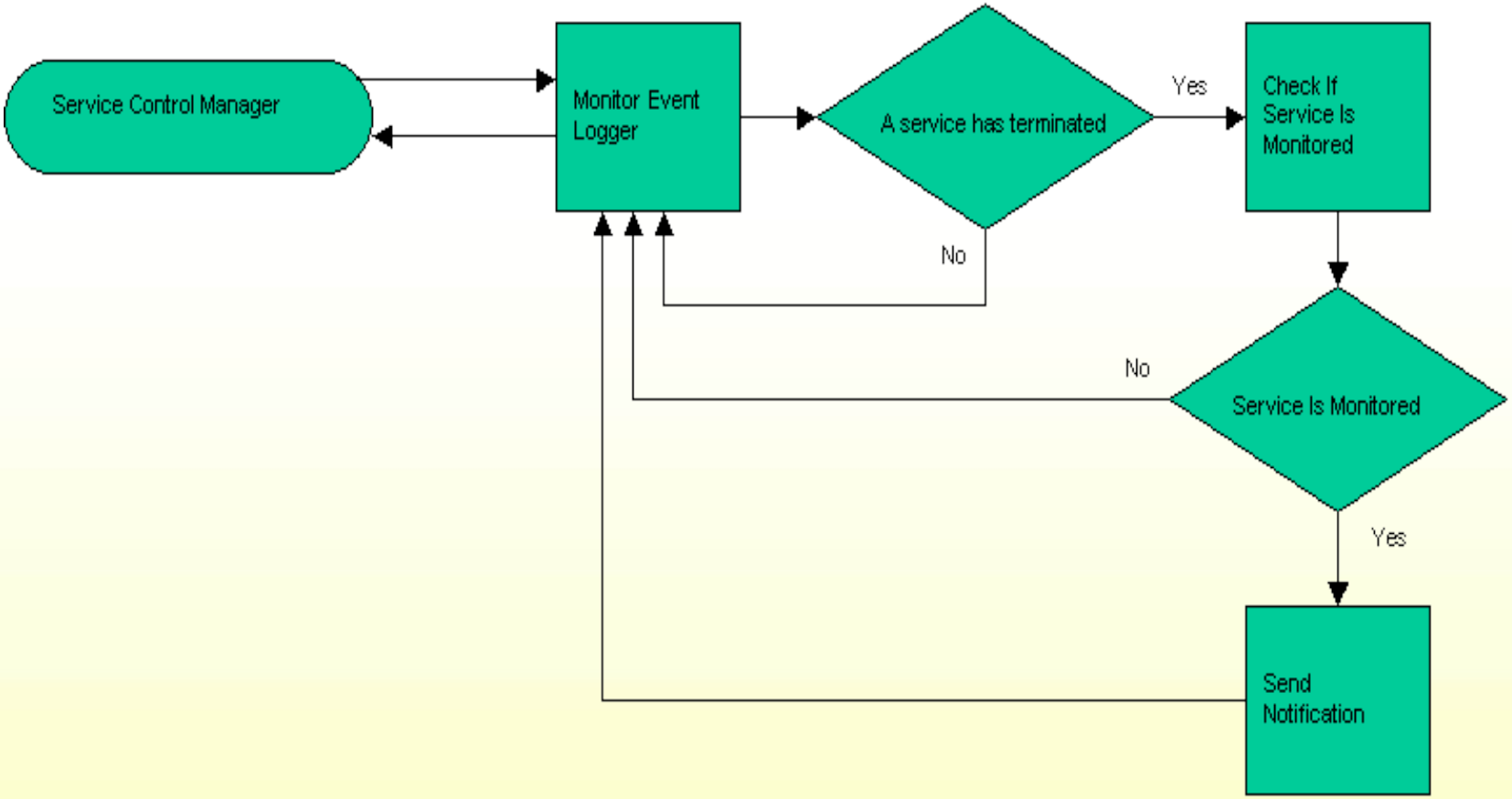
- Ability to monitor a service for failures
- Display a notification to the user
- Start services in a particular order
- Send email notification to a user

Watchdog

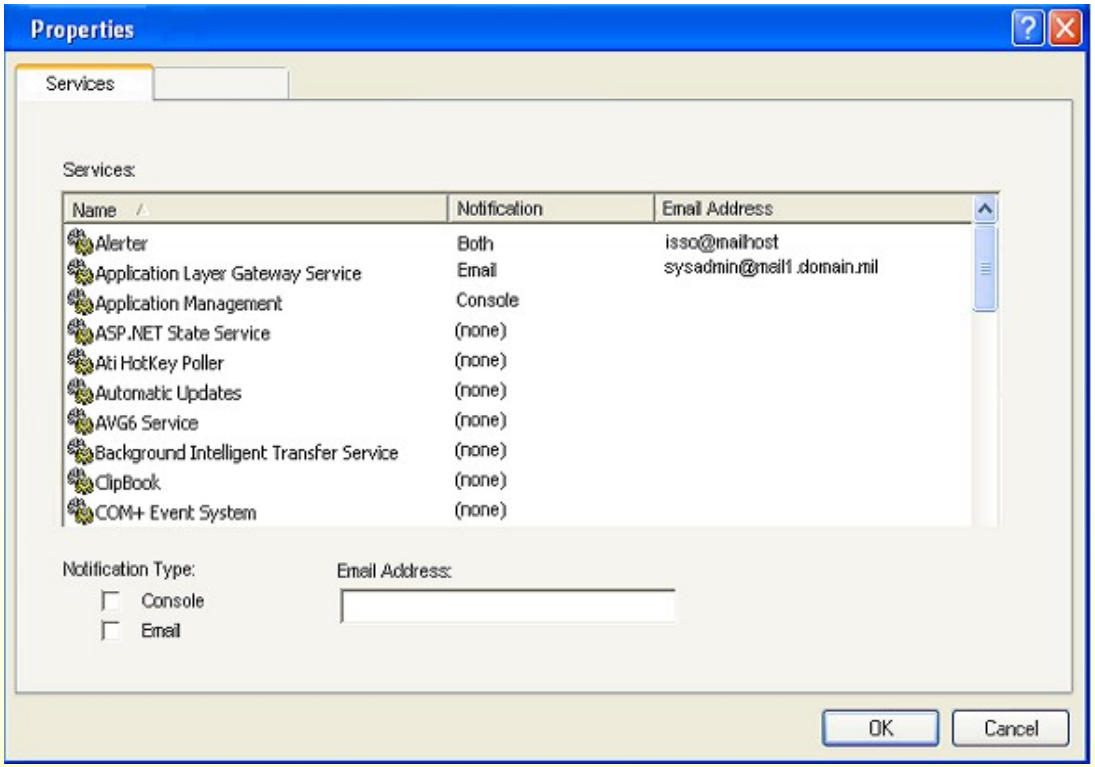
Proposed Functionality

- Windows provides all of the functionality that Watchdog provides except the ability to send email notifications
- Watchdog will now monitor the Event Log to determine when a service fails
- Upon detecting a failed service Watchdog will send the user notification either through email or an on screen dialog
- The on screen dialog will support terminal services

Watchdog Processing Diagram



Watchdog



- The Service tab allows the user to configure notification for the services available
- User is provided with a list of all services available. The chart shows the current configuration for each service
- User can select multiple entries to assign the same options for those services
- Multiple email addresses can be specified in the “Email Address” text field. The list of email

Questions

Questions???

Print Utility

Purpose

The Windows Print Utility provides the ability to print security classification markings on all printed output.

Current Functionality

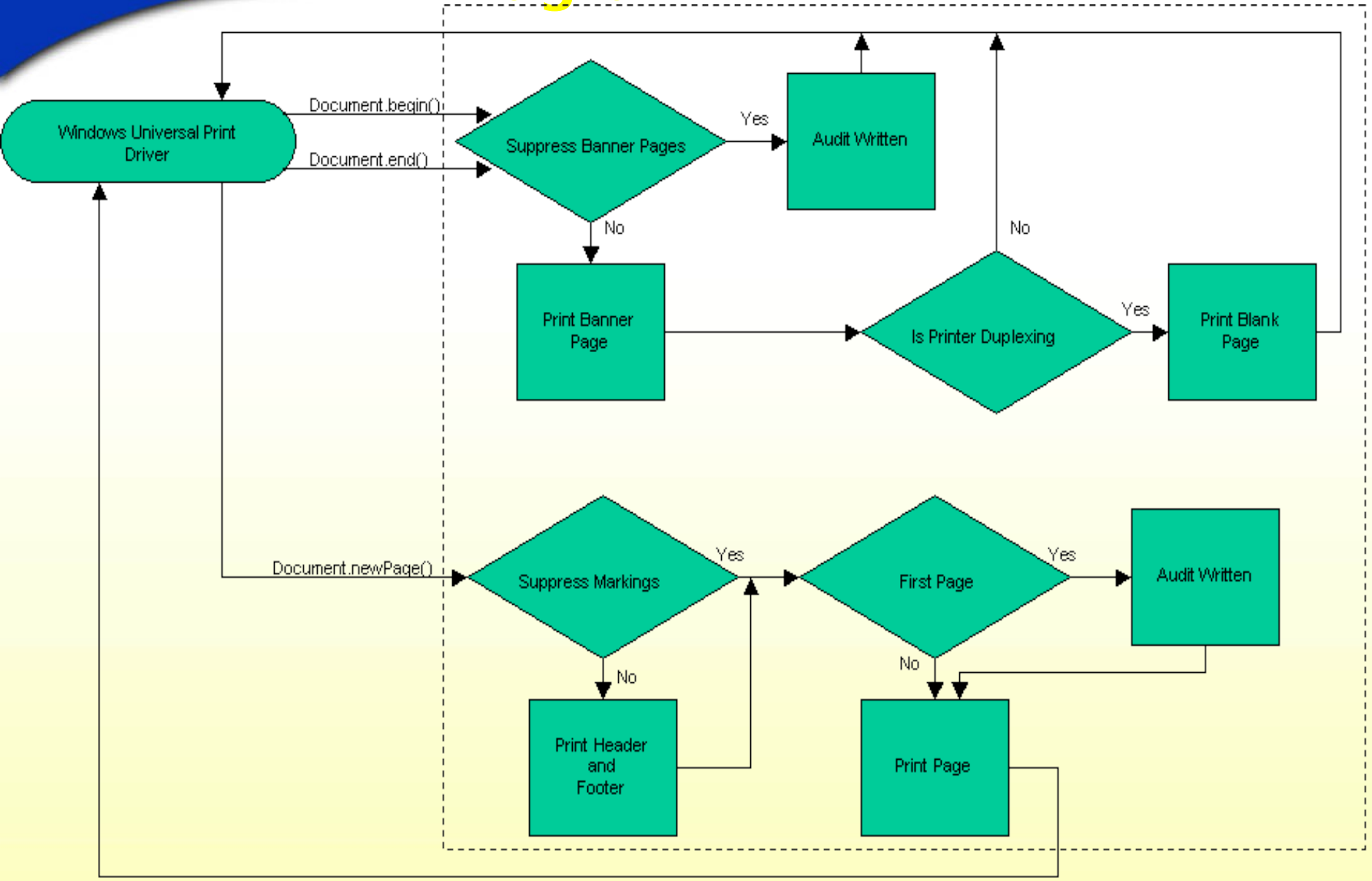
- Configurable Handling Instructions, Caveats, Code Words, Classification Markings
- Configurable System High label and short label
- Print banner pages on postscript printers
- Print security markings on all pages on postscript printers
- Ability to suppress banners and/or markings

Print Utility

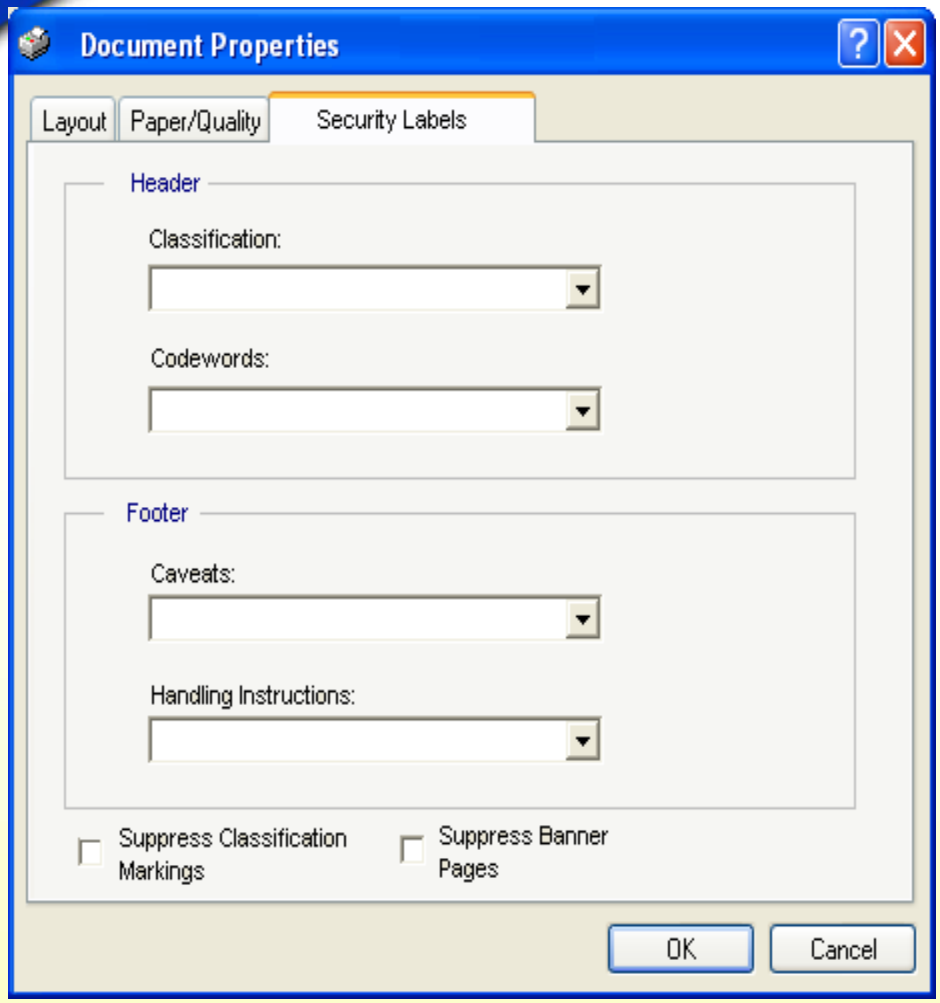
Proposed Functionality

- Print banner pages and security markings on PCL printers
- Ability to prepend “For demonstration purposes only” to security markings
- Creations of roles to limit which users can suppress banners/markings, select available markings, and enter custom markings
- Non-interactive installation
- Support for print servers
- The Print Utility will be created as a user-mode print driver
- This will allow the utility to modify the print stream in real-time

Print Utility Processing Diagram

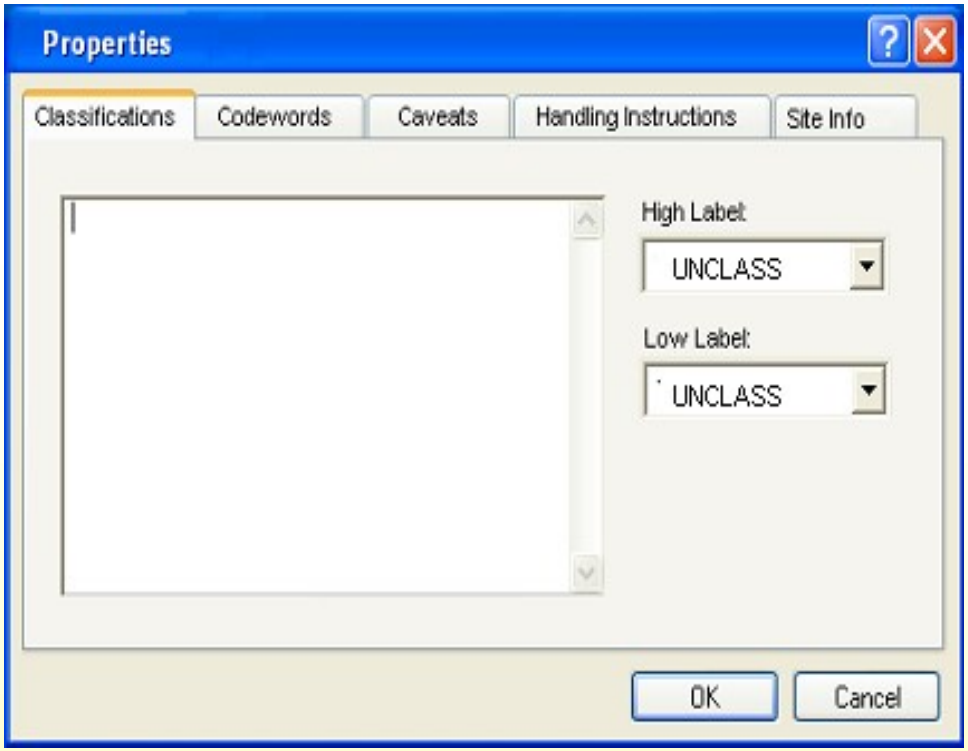


Print Utility



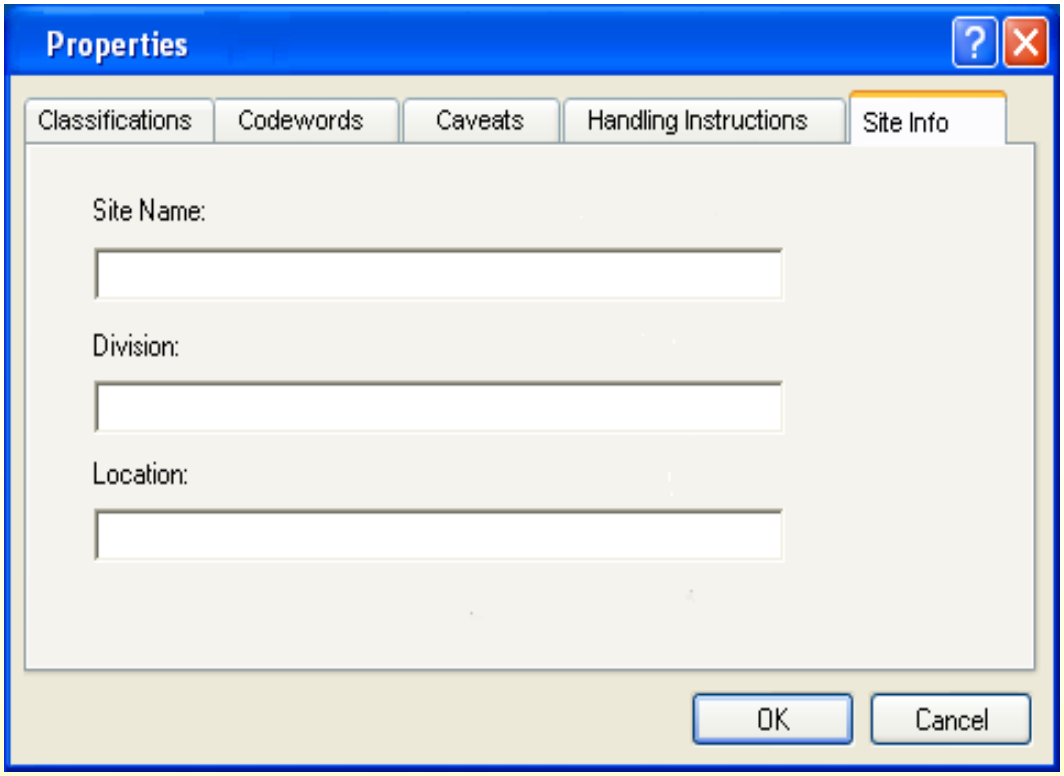
- Configuring the security markings on the printed output shall be handled by a new tab created on the printer properties screen.
  Privileges will be divided into three levels:
  NONE - Will not be able to modify the security banner or markings on printed output
  LOW - Will be able to select Classification, Codewords, Caveats, and Handling Instructions from the drop-down, but will not be allowed to suppress banner pages or security markings
  HIGH - No limitations are imposed on the user

Print Utility



- The first four tabs allow the user to enter Classifications, Codewords, Caveats, and Handling Instructions. Each entry will be separated by a new-line character
- This panel is called from the JMC console

Print Utility



- The last tab allows the site to change the name, division, and location of the site
- This panel is called from the JMC console

Questions

Questions???

Event Backup

Purpose

The purpose of Event Backup is to collect logs from machines on a network for storage in a central location. The Event Backup implementation for JEDI 2.0 is detailed in this design specification.

Current Functionality

- Event backups occur every day at approximately 12:00 AM This time is not configurable
- The logs that are collected are not configurable, and are currently limited to only the security log
- Event Backup runs as a service
- There is no timeout on downloads
- Event logs are always cleared after a download is completed
- Only runs on a domain controller

Event Backup (Cont.)

Proposed Functionality

The Event Backup utility for the JEDI 2.0 release has been changed to be more versatile and useful. The new design seeks to make the Event Backup Utility easier to use and more useful through the use of a GUI based configuration utility with a flexible backup scheduler.

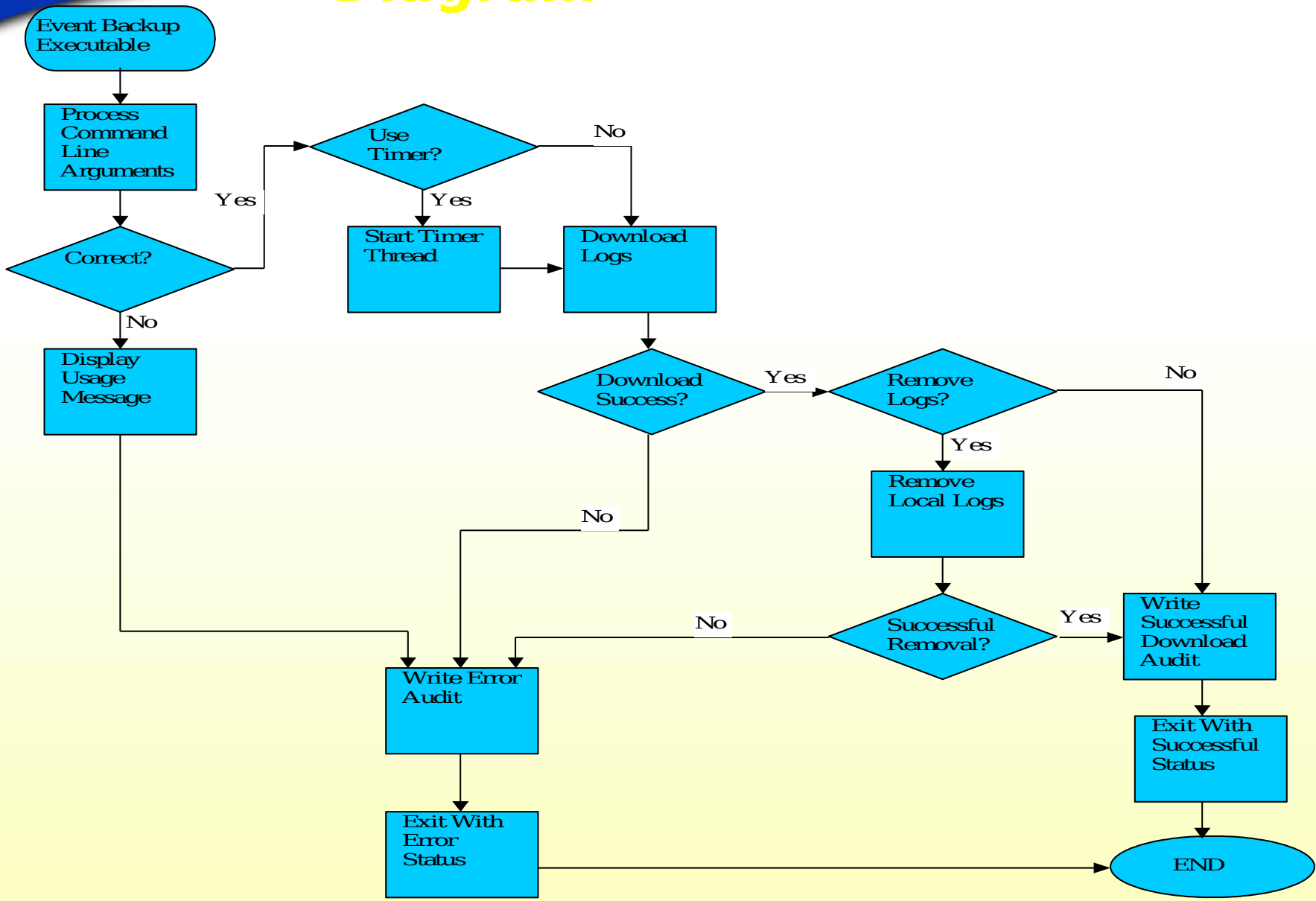
- Ability to collect any log that exists on the system, including security, system, and application logs
- Ability to form groups of hosts to be scheduled together
- Easy configuration through a GUI based snap-in for the MMC
- All settings are stored in the registry

Event Backup (Cont.)

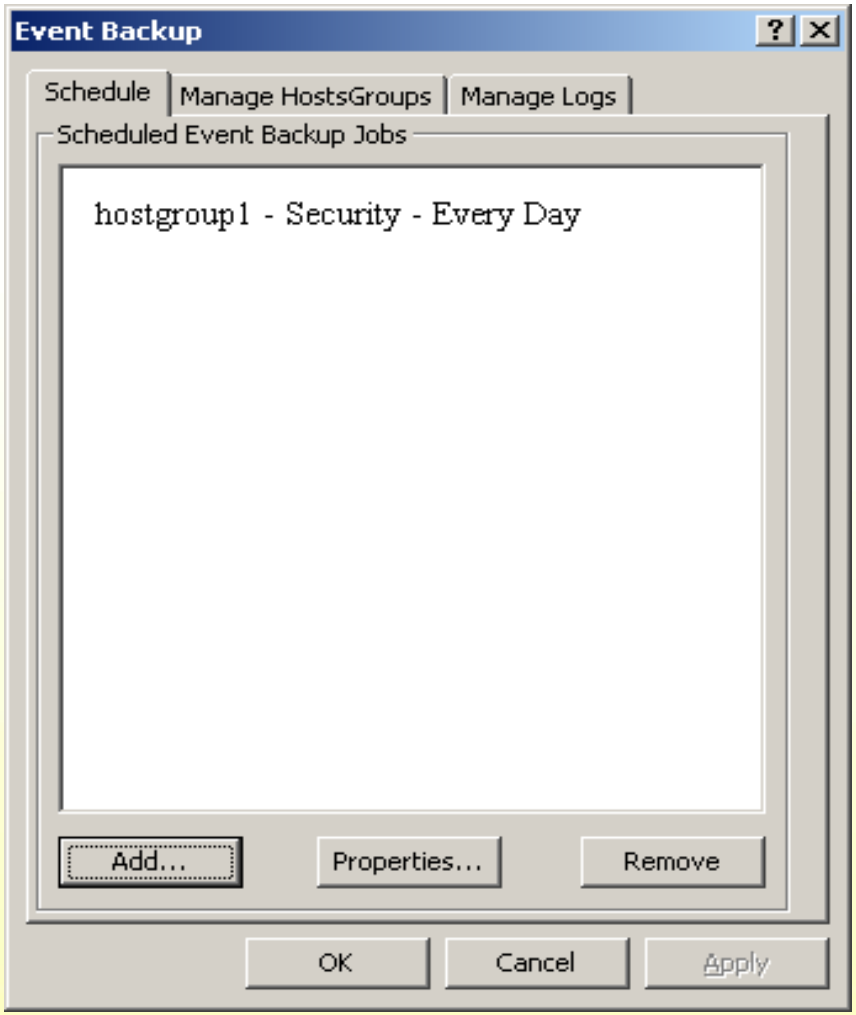
Proposed Functionality (cont.)

- Able to work in a mixed environment of Windows 2000/XP/2003
- Ability to schedule event backups to occur at any time
- Support Terminal Server (Remote Desktop)
- Will not need to be on a domain controller to run (if determined to be technically feasible)
- The Event Backup Executable gets necessary information from the arguments passed in via the command line. This information consists of host groups, hostnames, log and archive locations, timeout information, and optionally clearing local logs after download
- Add Hosts to a Group to create HostGroups

Event Backup Processing Diagram



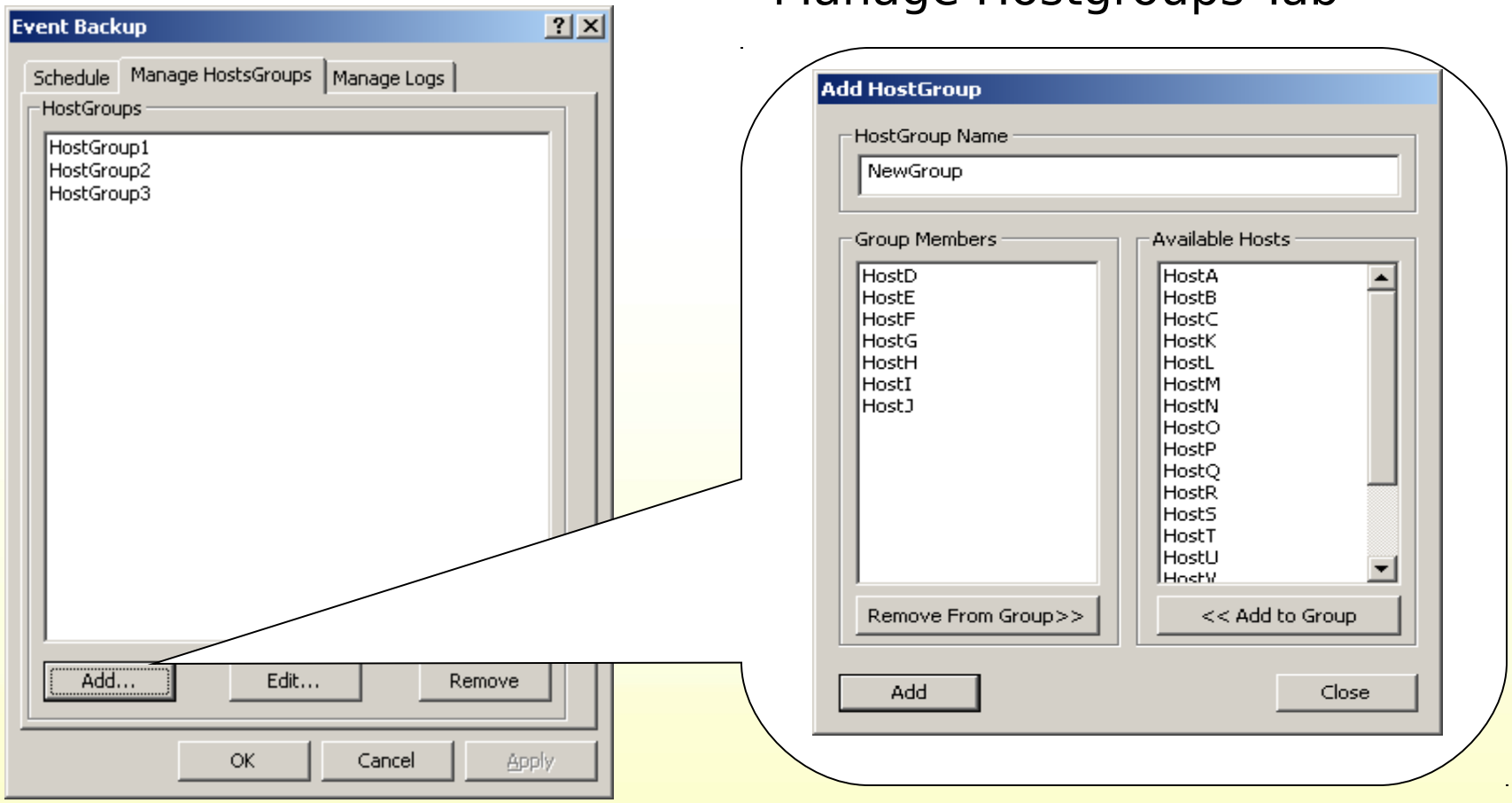
Event Backup Schedule Tab



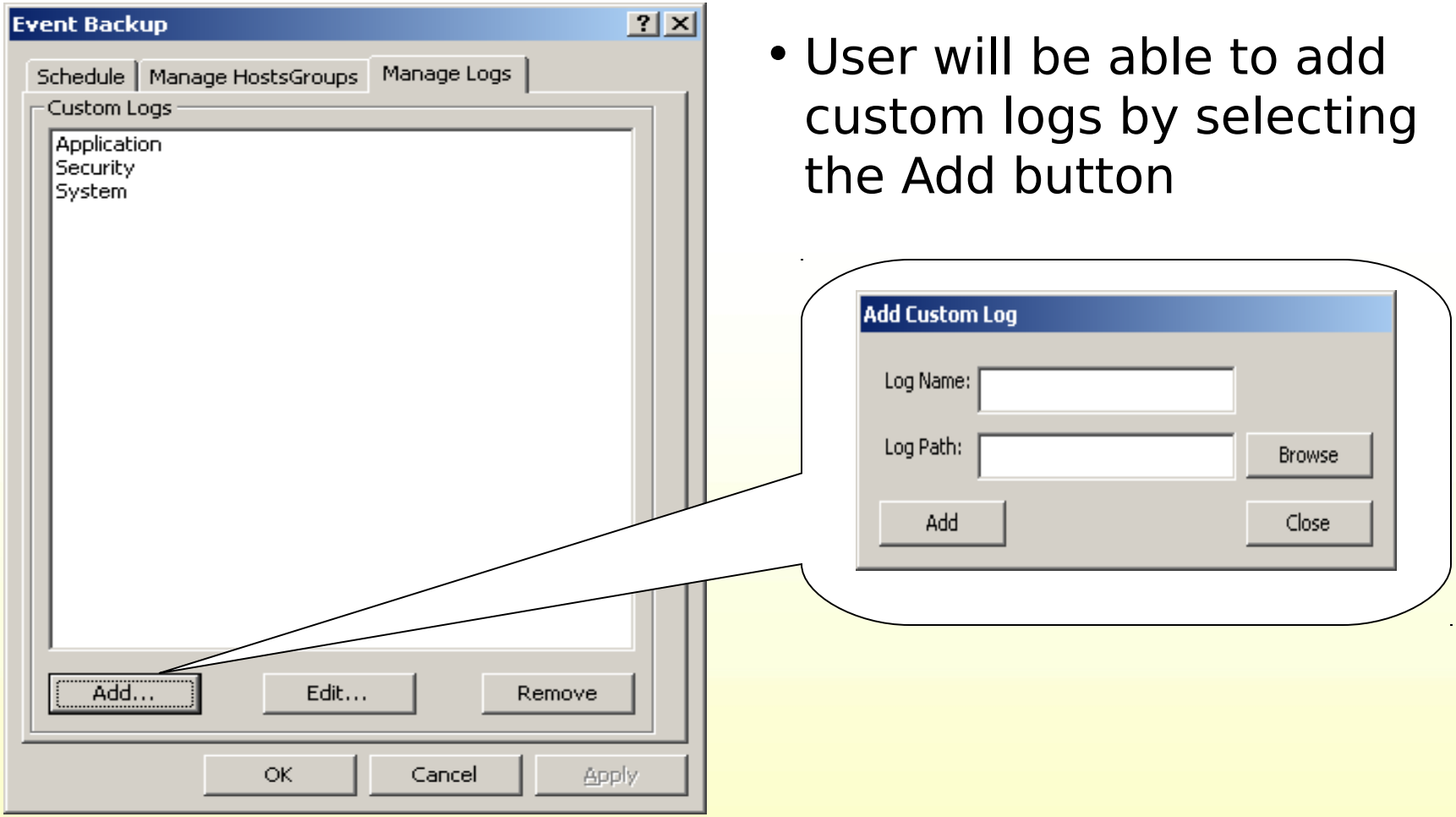
- In JEDI 2.0, the user will be able to schedule downloads with a great deal of flexibility
- The user can schedule downloads to occur hourly, daily, weekly, monthly, or one time only
- This dialog has the ability to add and remove jobs through a wizard when selecting the Add button
- This panel is called from the JMC console

Event Backup HostGroups Tab

- Manage Hostgroups Tab

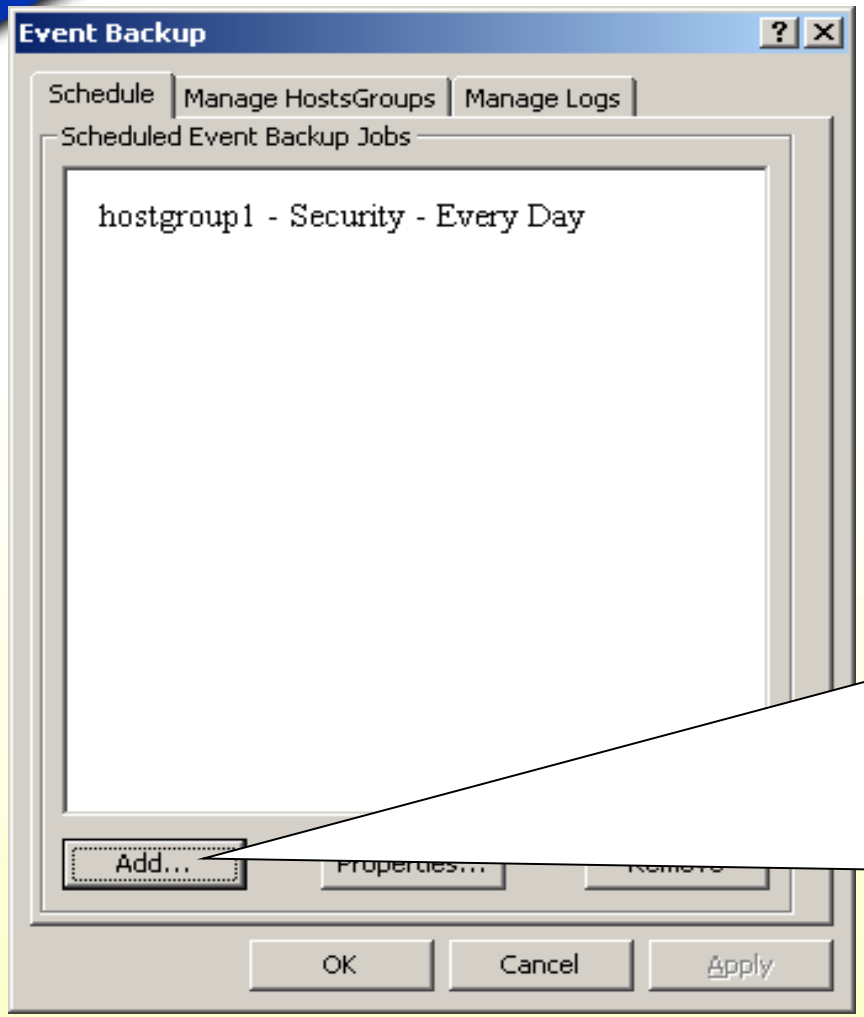


Event Backup Manage Logs Tab

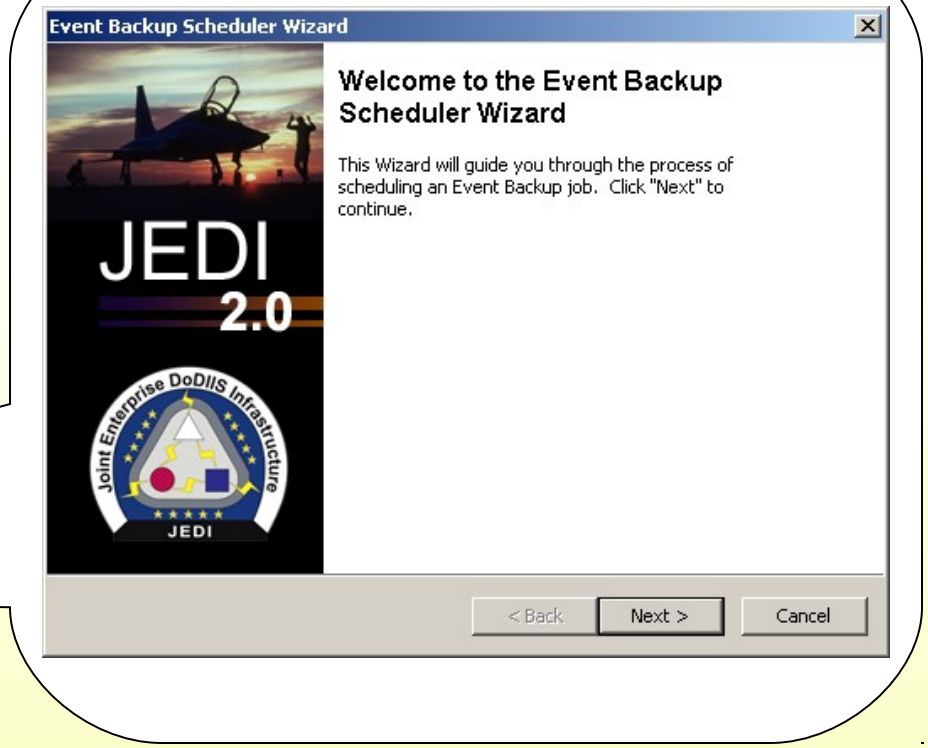


- User will be able to add custom logs by selecting the Add button

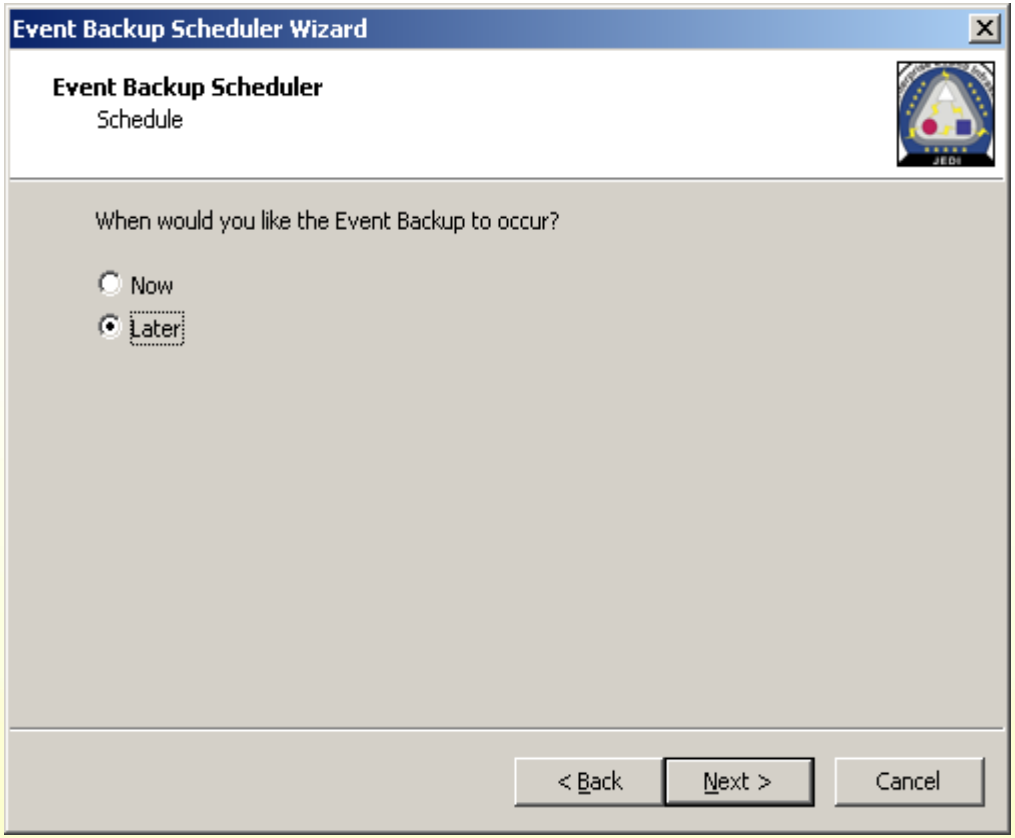
Event Backup Scheduler Wizard



- Selecting Add will begin the Schedule Wizard

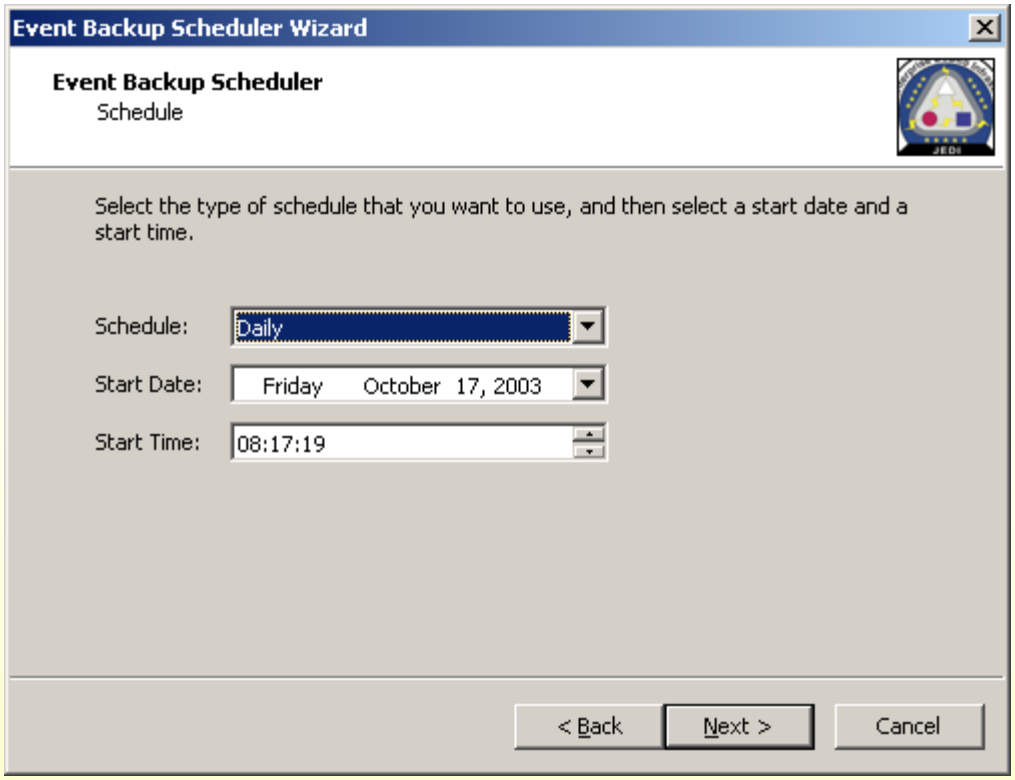


Event Backup Scheduler Wizard



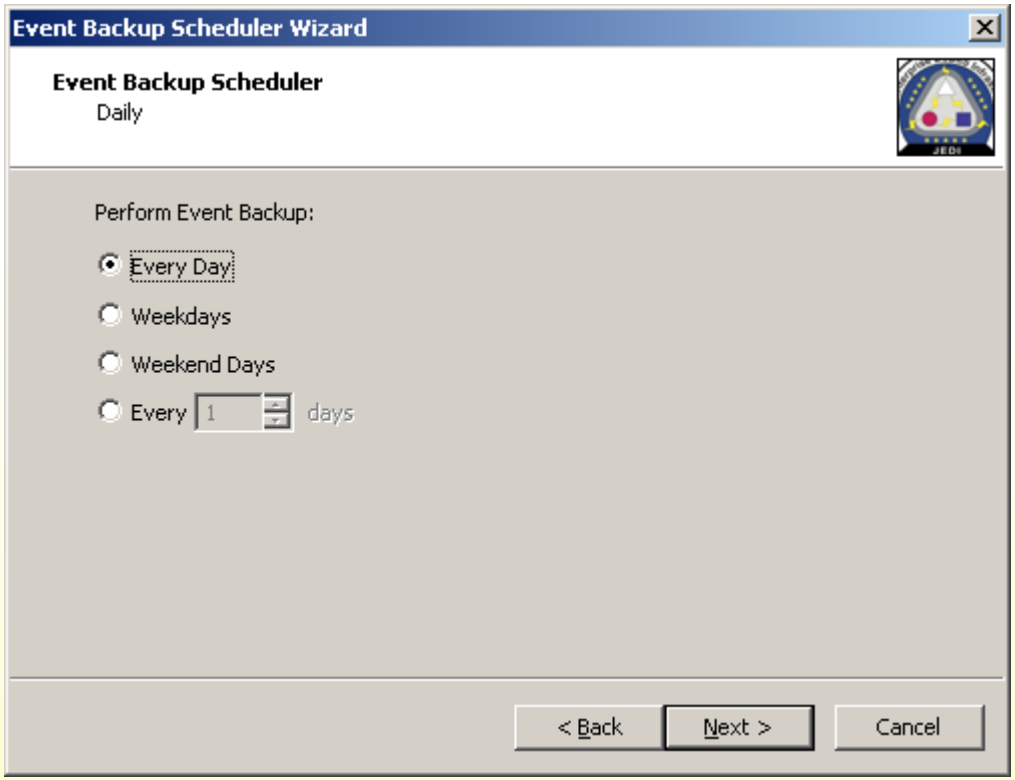
- On-demand Download or Schedule to Run Later

Event Backup Scheduler Wizard



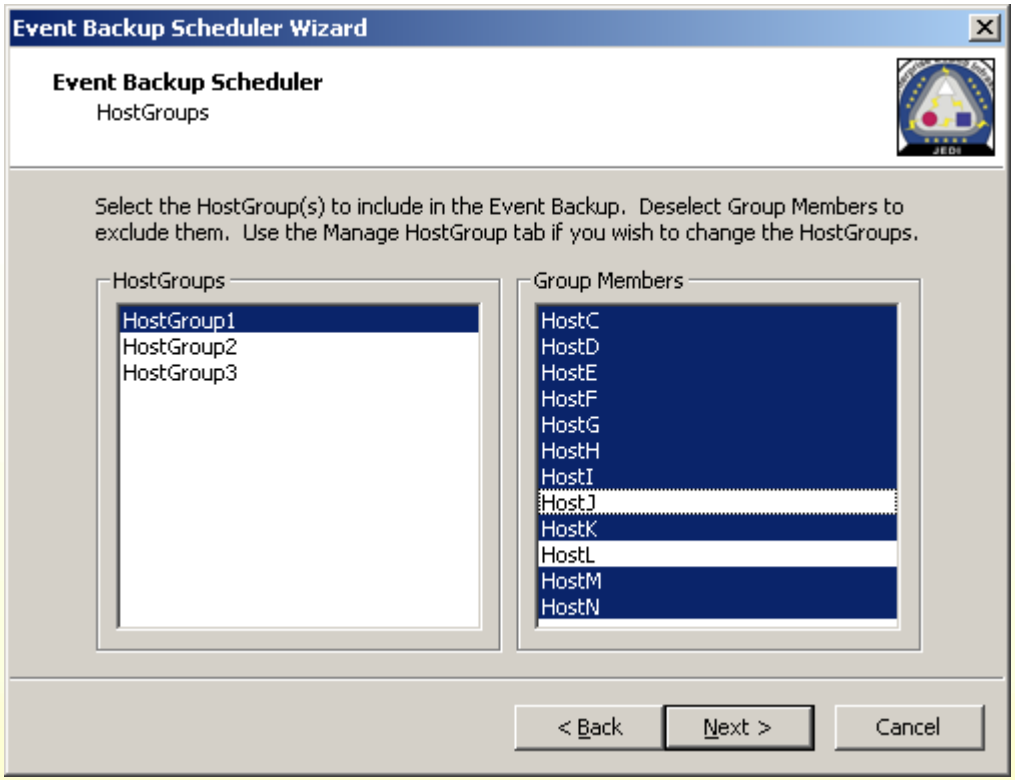
- Schedule Type, Start Date and Time

Event Backup Scheduler Wizard



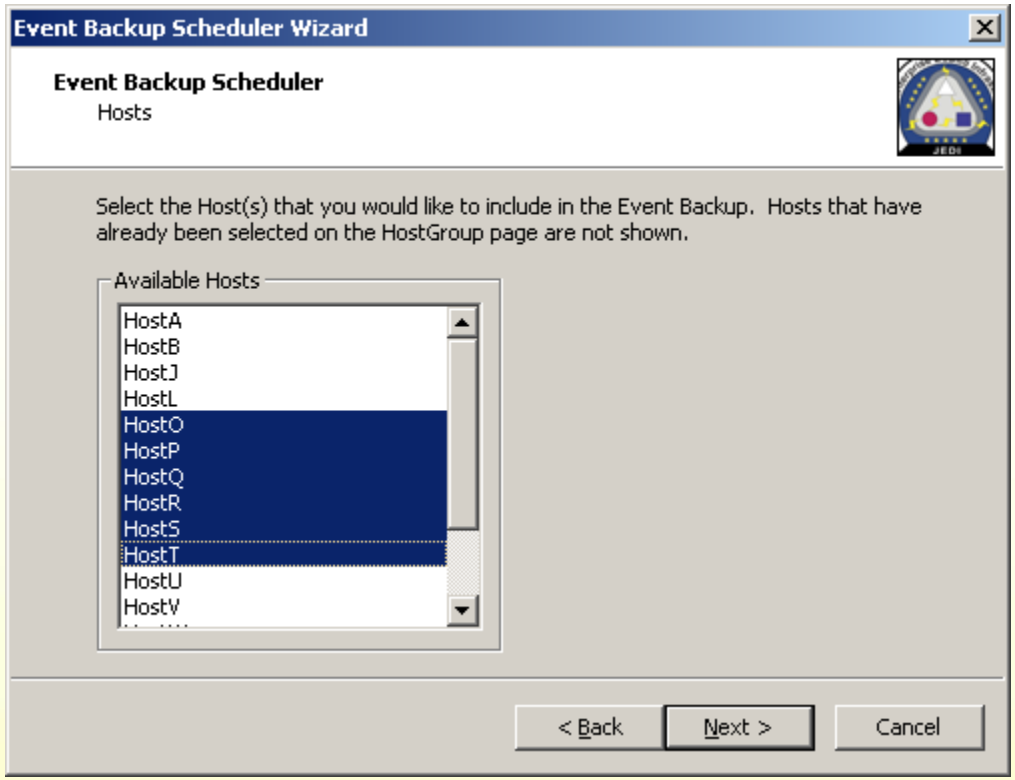
- Daily Options

Event Backup Scheduler Wizard



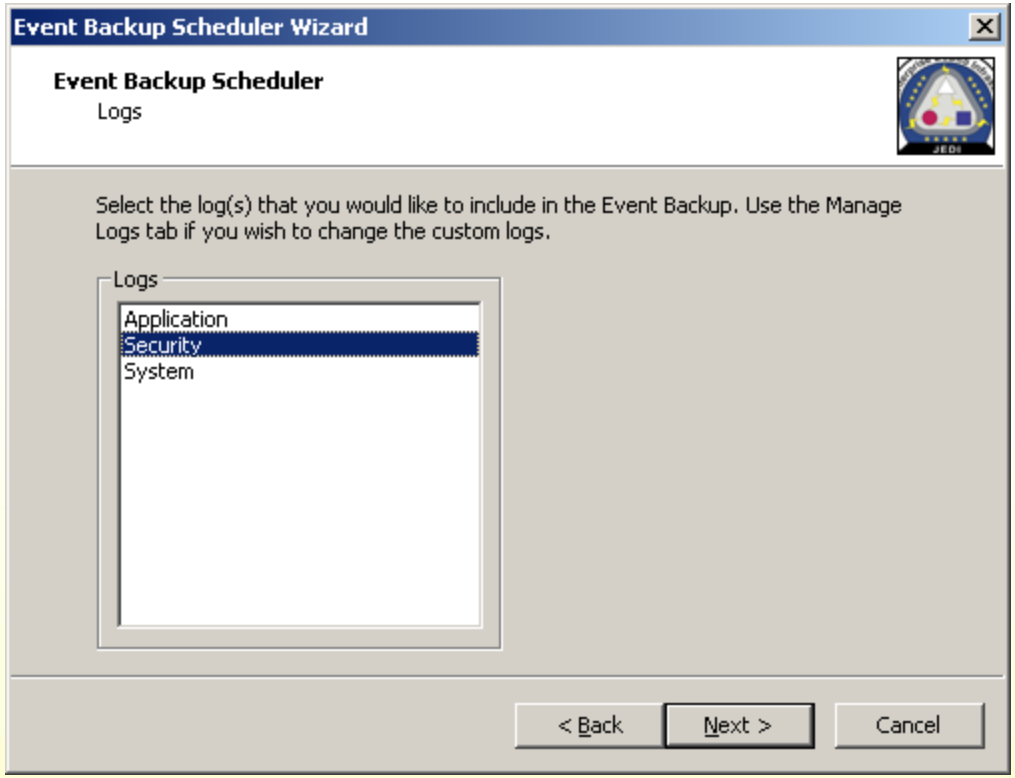
- Ability to Select HostGroups and exclude/include Group Members

Event Backup Scheduler Wizard



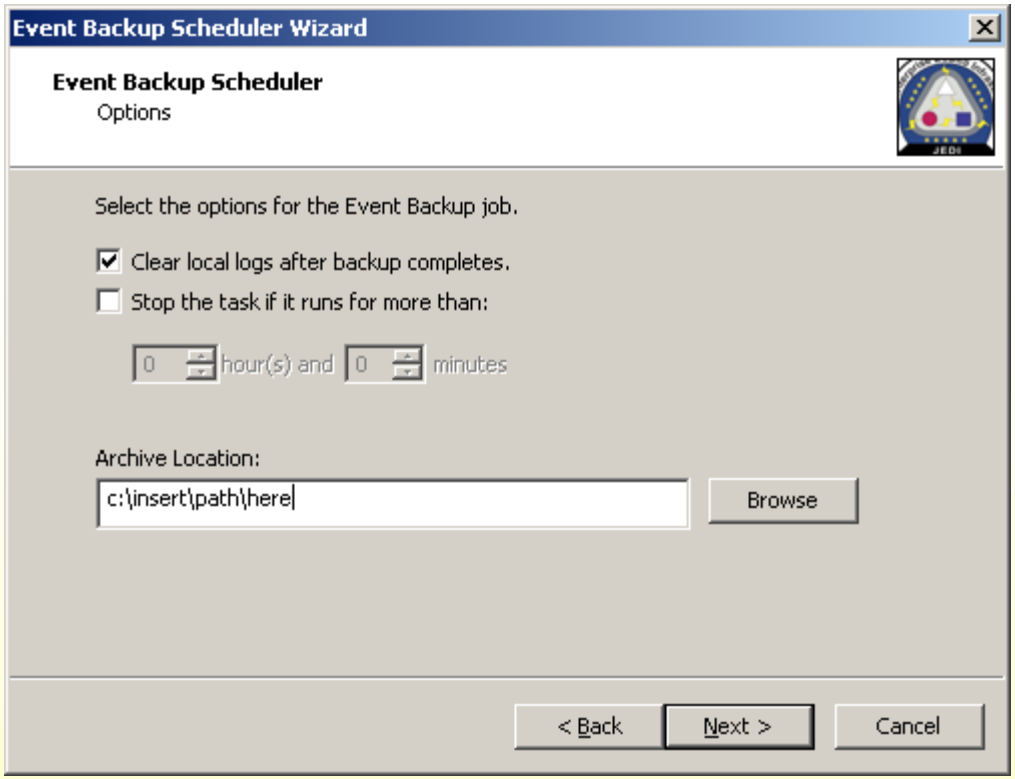
- Ability to Select Individual Hosts

Event Backup Scheduler Wizard



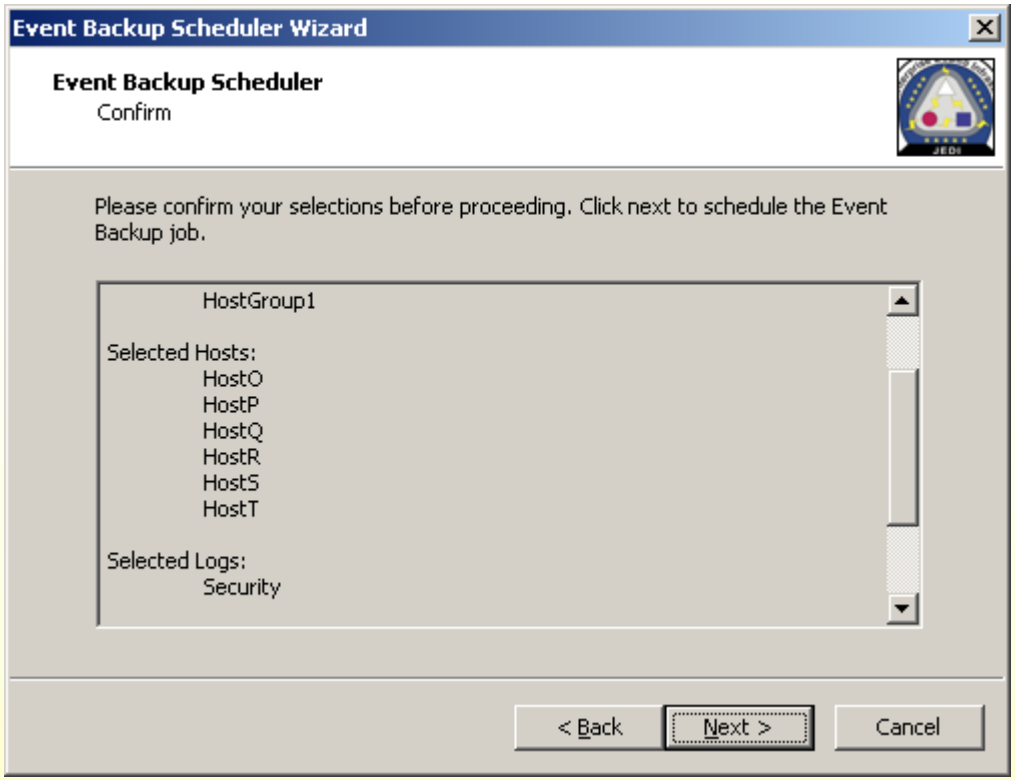
- Ability to select Log files to be downloaded

Event Backup Scheduler Wizard



- Ability to select Event Backup options

Event Backup Scheduler Wizard



- Confirm final results before proceeding

Event Backup Scheduler Wizard

- Finished adding scheduled job

Questions

Questions???

Clear Temp

Purpose

The Clear Temp utility clears files from the temporary directory at logout.

Current Functionality

- Executes at logon via the Run Registry key
- Cannot be disabled or killed by users
- Obtains temp directory path from environment
- Executes only under user context
- Configured via system environment settings
- Current process order
    1. Executes at login
    2. Sleeps until logout event
    3. At logout event, clears “TEMP” directory

Clear Temp

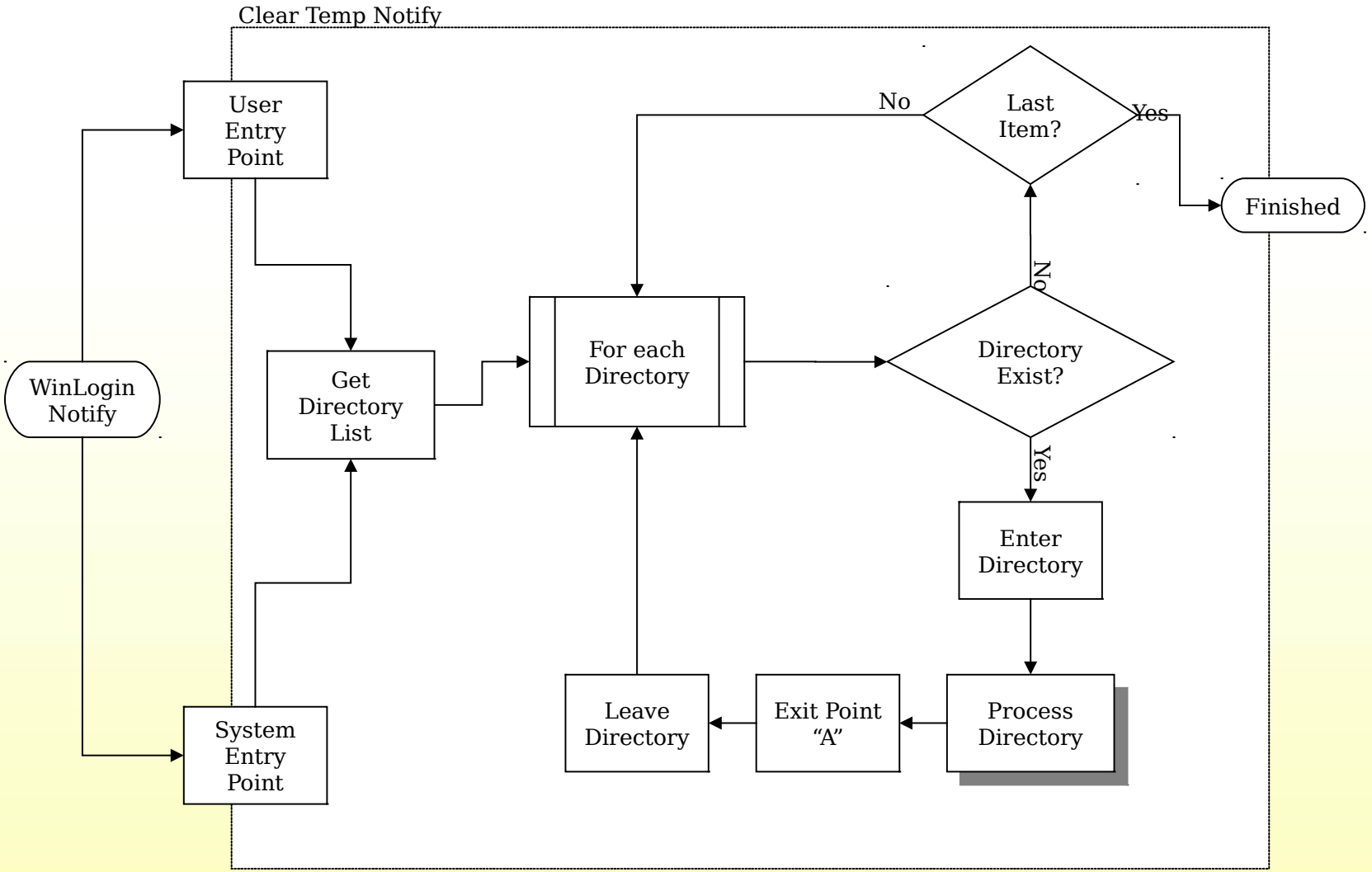
Proposed Functionality

The Clear Temp utility should always execute on a session logout. This functionality is expanded with a configurable option to execute at login. Northrop Grumman will supply a MMC snap-in GUI to facilitate this configuration.

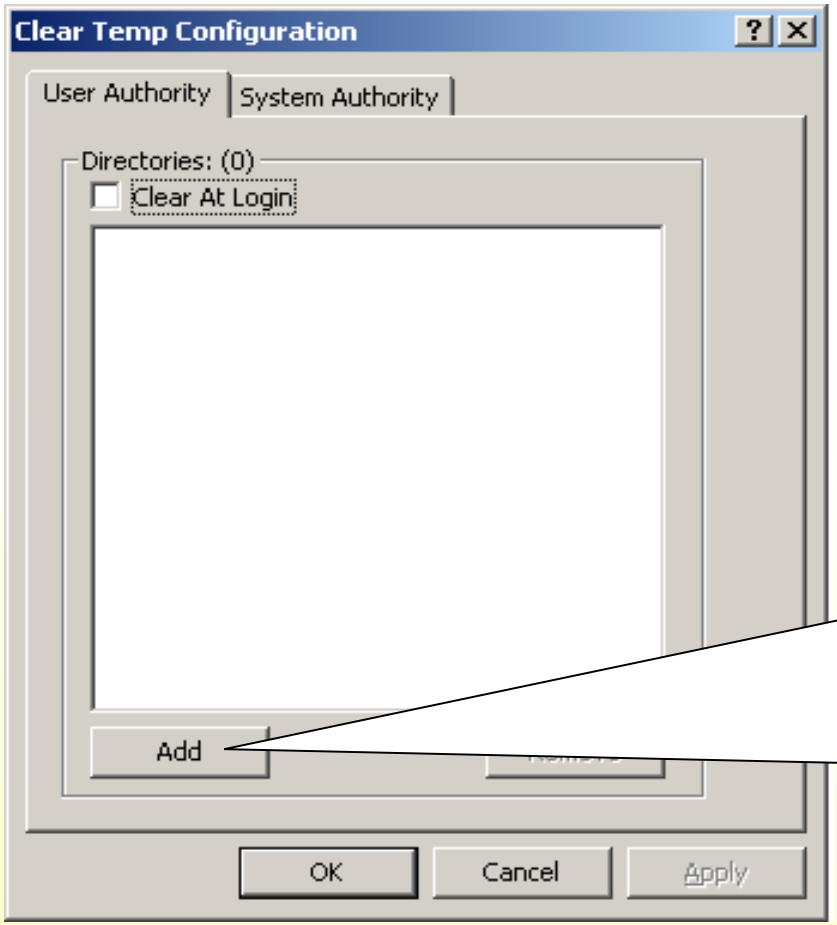
A summary of this functionality:

- Cannot be disabled or killed by user
- Always execute at logout
- Optional execution at login
- Obtains “temp” directory paths from registry
- Configurable list of directories
- Executes in both user context and admin context
- Configurable from a MMC GUI
- Must support Terminal servers
- Deadman interoperability

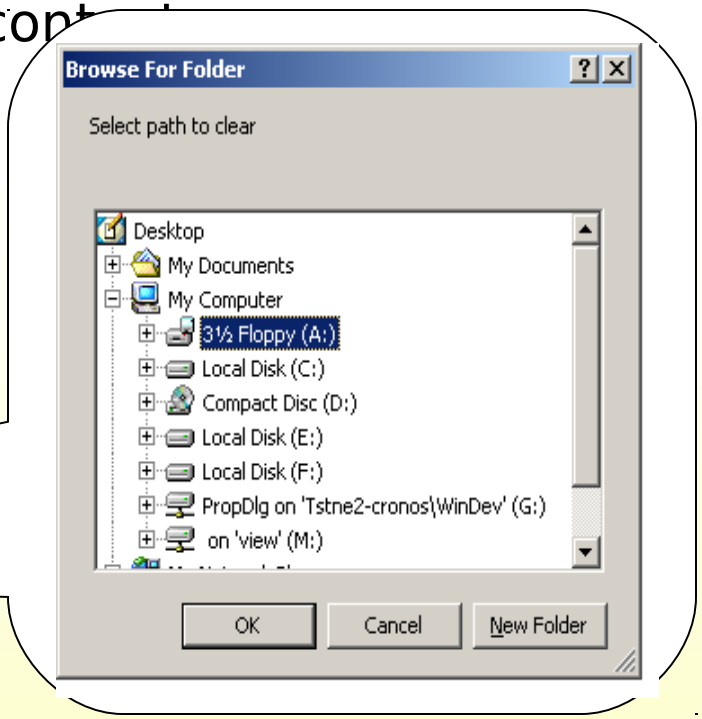
Clear Temp Processing Diagram



Clear Temp

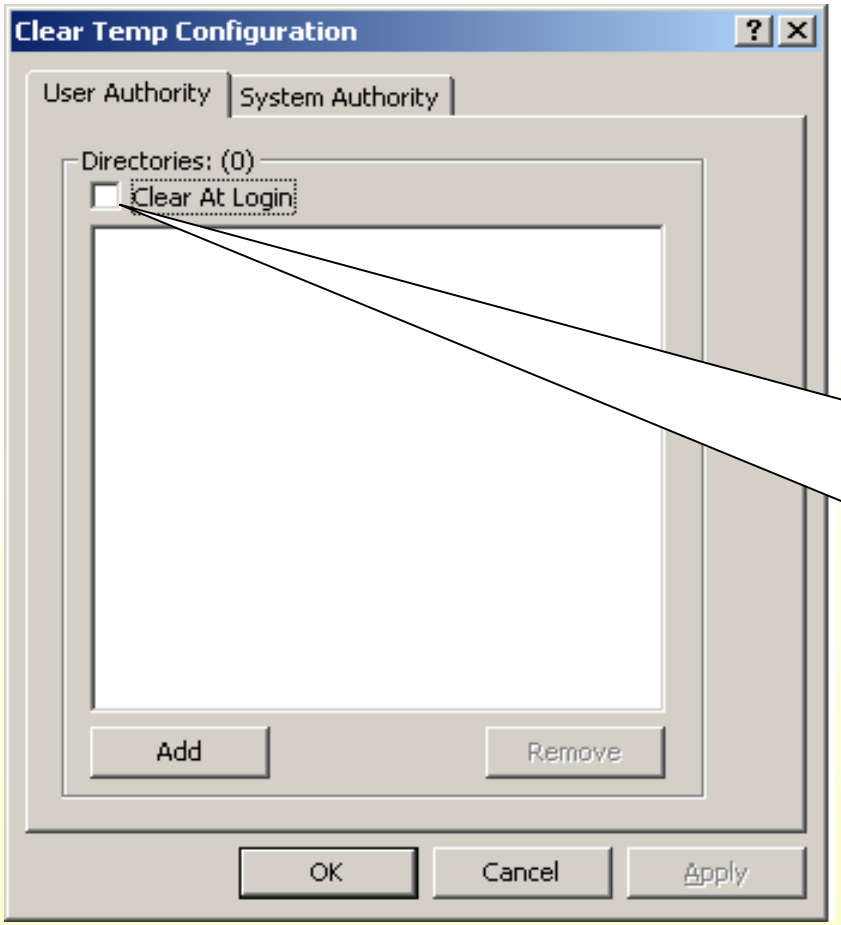


- The functionality of the Add and Remove buttons are the same for both the Users Context area and the System cont

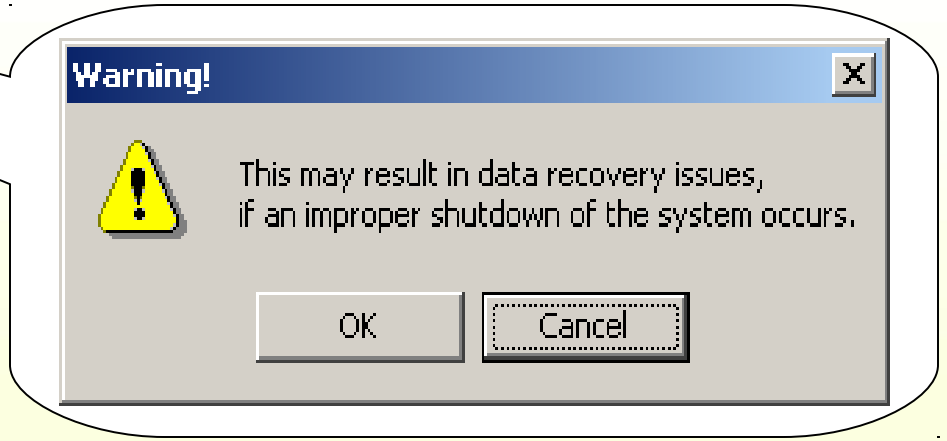


- When the “Add” button is pressed, a standard Microsoft file browser will appear

Clear Temp



- When the user selects the “Perform at login” option, the following warning message will appear



Questions

Questions???

Deadman

Purpose

Deadman provides the capability to perform an action(logoff, notification, etc) when a users screen saver has been active for a configured amount of time.

Current Functionality

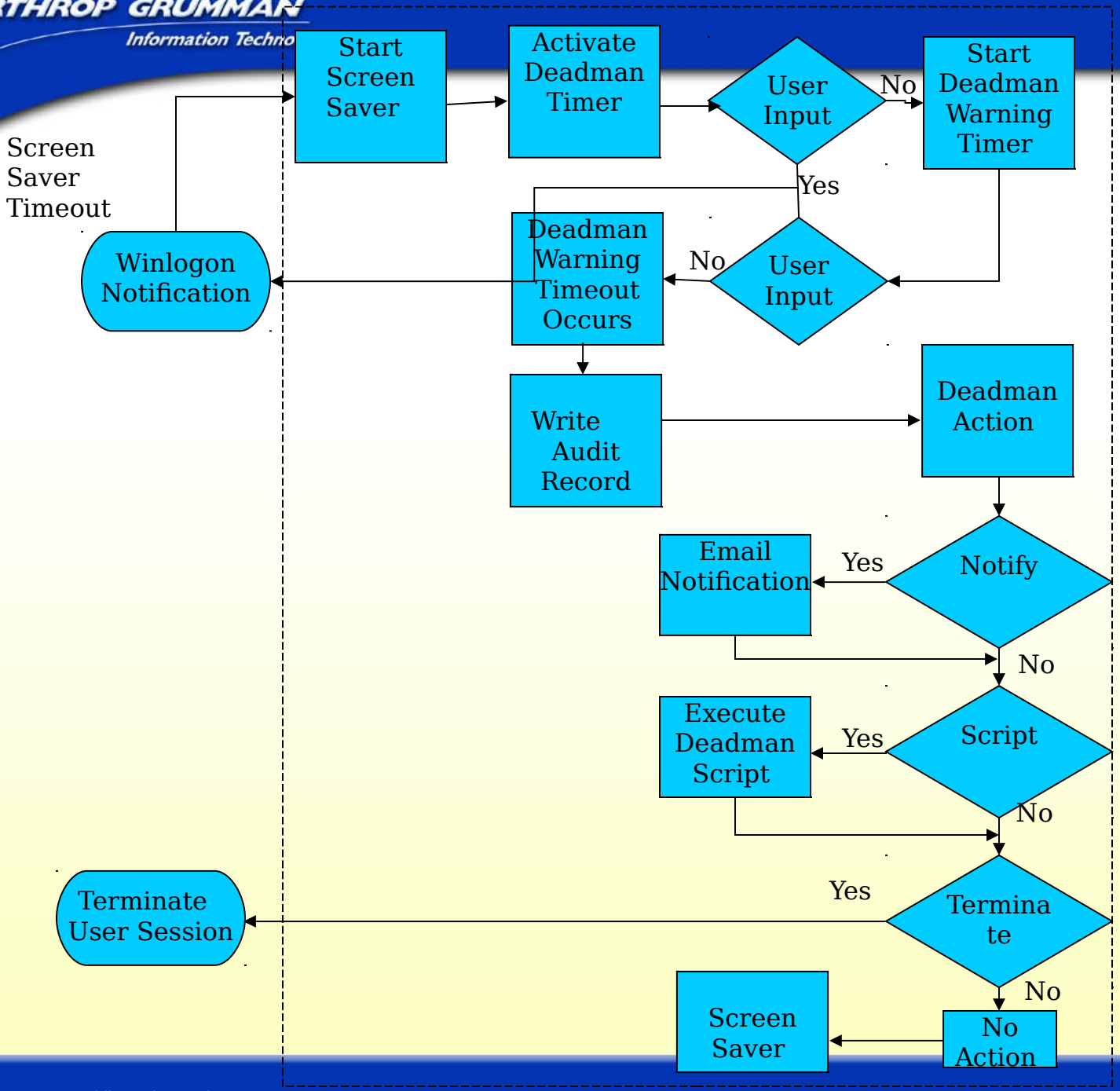
Deadman provides the current functionality:

- Deadman runs as a background process periodically checking for an active screensaver
- Windows 2000 systems with configuration properties being stored in the flat file “deadman.conf”

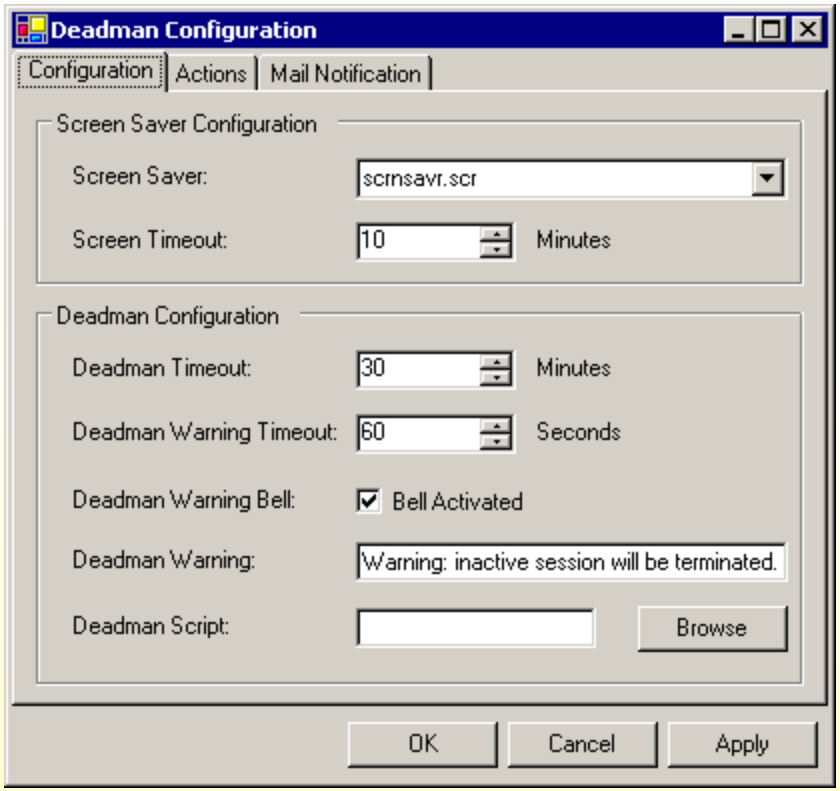
Deadman

Proposed Functionality

- The configuration settings will be stored in the registry
- Deadman utility will also be implemented as a Windows DLL or a Screensaver
- More familiar and intuitive interface to configuring Deadman utility using the JMC through the MMC console
- Systems accessed through Windows Terminal Services benefit from Deadman functionality

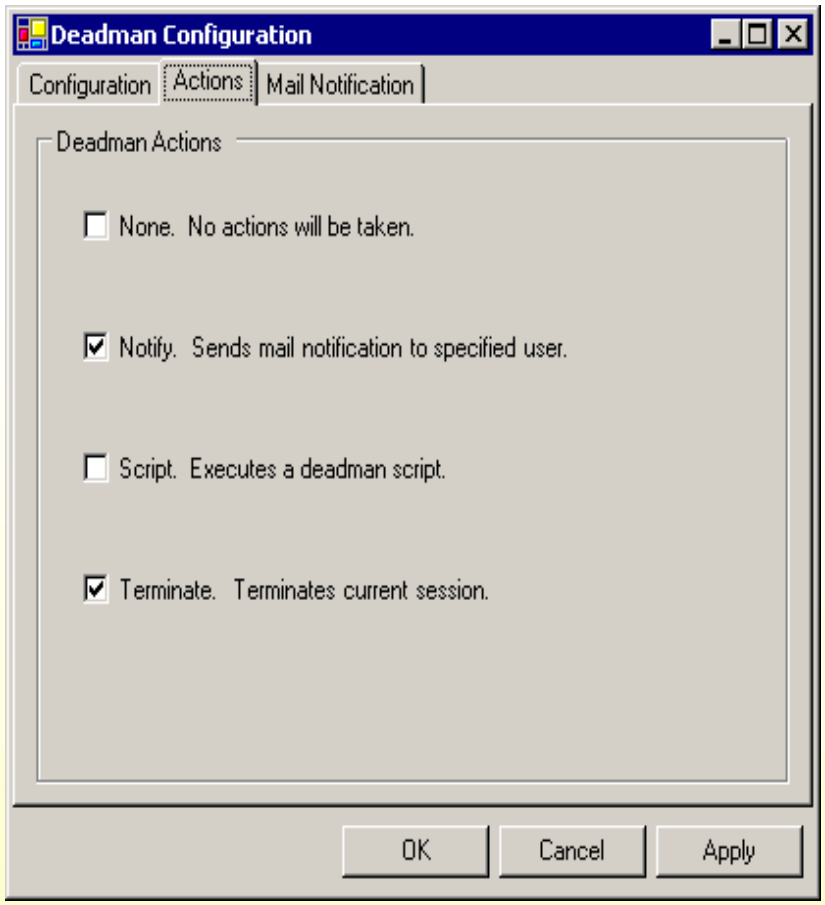

Start Screen Saver
Activate Deadman Timer
User Input
No
Start Deadman Warning Timer
Yes
Screen Saver Timeout
Winlogon Notification
Deadman Warning Timeout Occurs
No
User Input
Write Audit Record
Deadman Action
Email Notification
Yes
Notify
No
Execute Deadman Script
Yes
Script
No
Terminate User Session
Yes
Termina te
No
Screen Saver
No Action

Deadman



- Screen Saver Timeout. The screen saver will appear after this timeout has expired
- Deadman Timeout. Deadman's warning timeout will start after this timeout has expired
- Deadman Warning Timeout Deadman's action will occur after this timeout has expired
- Deadman Warning Bell. Selecting this activates a warning bell sound that is played during the Deadman Warning timeout
- Deadman Script. The name of the script that will be executed after the Deadman Warning timeout expires

Deadman



- None. No actions will be taken after the Deadman warning timeout has expired
- Notify. A mail notification will be sent to a specified user after the Deadman warning timeout has expired
- Script. The specified script will be executed after the Deadman warning timeout has expired
- Terminate. The current user session will be terminated after the Deadman warning timeout has expired
- Deselecting all will result in No actions will be taken

Deadman

- Mail Recipient. The email address of the user who will receive the email notification when the notify action is set and the deadman warning timeout expires
- Mail Subject. The subject of the email that will be sent when the notify action is set and the deadman warning timeout expires
- Mail Server. The mail server that will be used to send the email notification when the notify action is set and the deadman warning timeout expires

Questions

Questions???

Logon Consent

Purpose

The Logon Consent Utility forces authenticated users to agree to a monitoring and usage agreement before given access to the system.

Current Functionality

Logon Consent currently provides the following functionality:

- Display a monitoring and consent message
- Allow a site to specify a custom message
- Display a window with a red background and white text
- Allow the user to accept or decline the agreement
- Timeout the transaction if the user does not select “Accept” or “Decline”
- Audit the action of the user
- Currently only a mouse selectable event

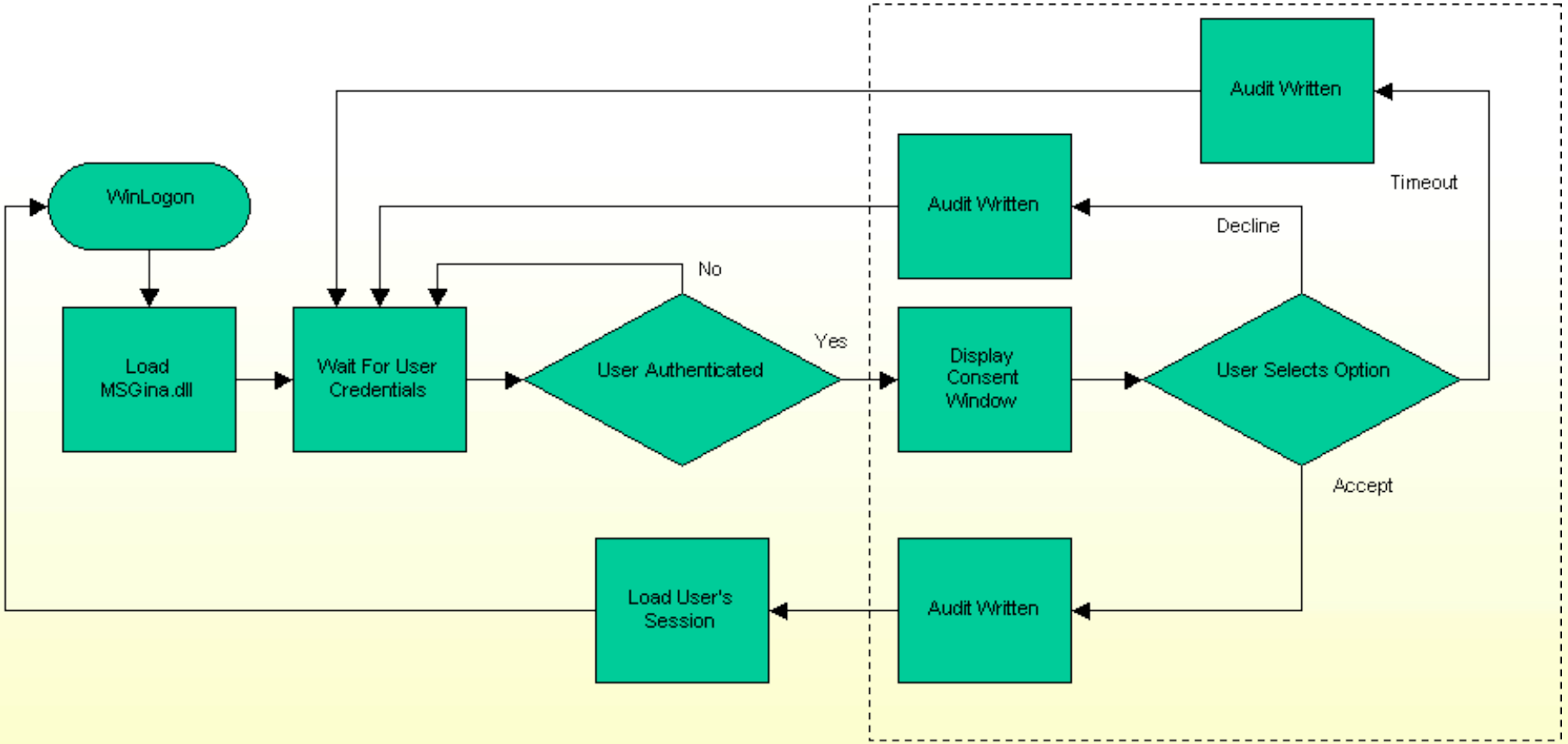
Logon Consent

Proposed Functionality

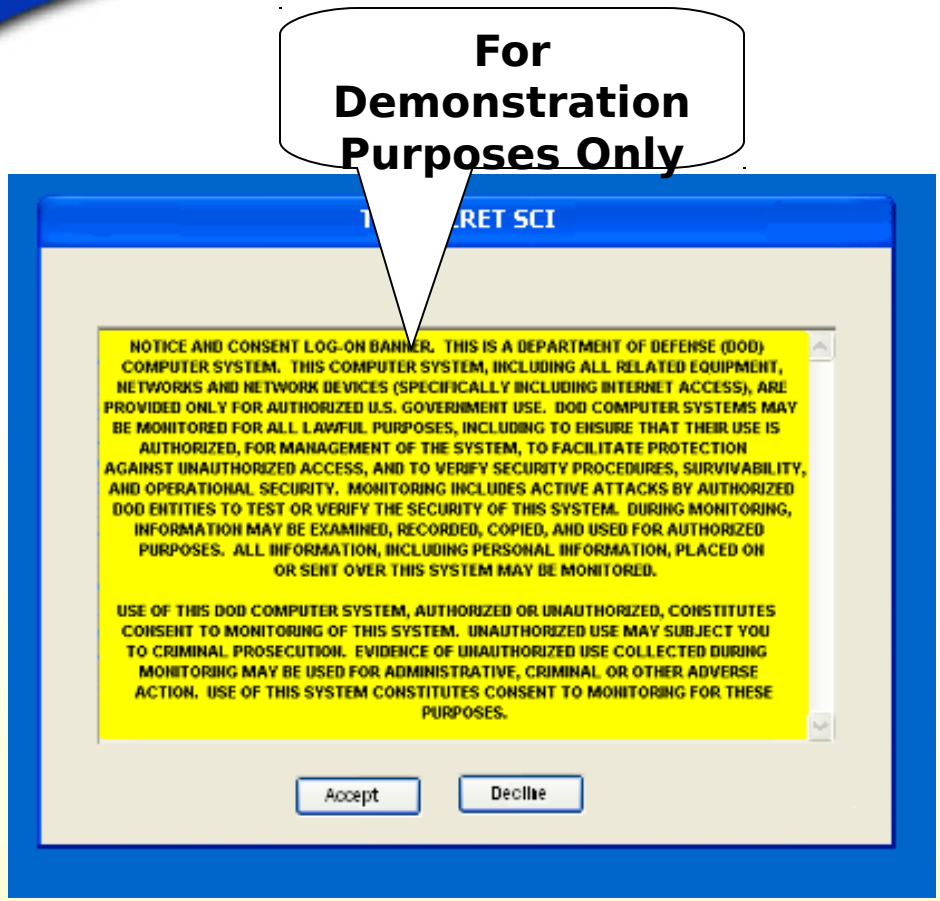
The following is proposed additional functionality for the Logon Consent Utility:

- Allow the background and text color to be configurable to match the classification of the workstation
- Allow all configuration to be done through a MMC snap-in
- Allow the user the ability to use the “Space” or “Enter” key accept the agreement
- It must support SmartCard support
- It must support Terminal Services

Logon Consent Processing Diagram

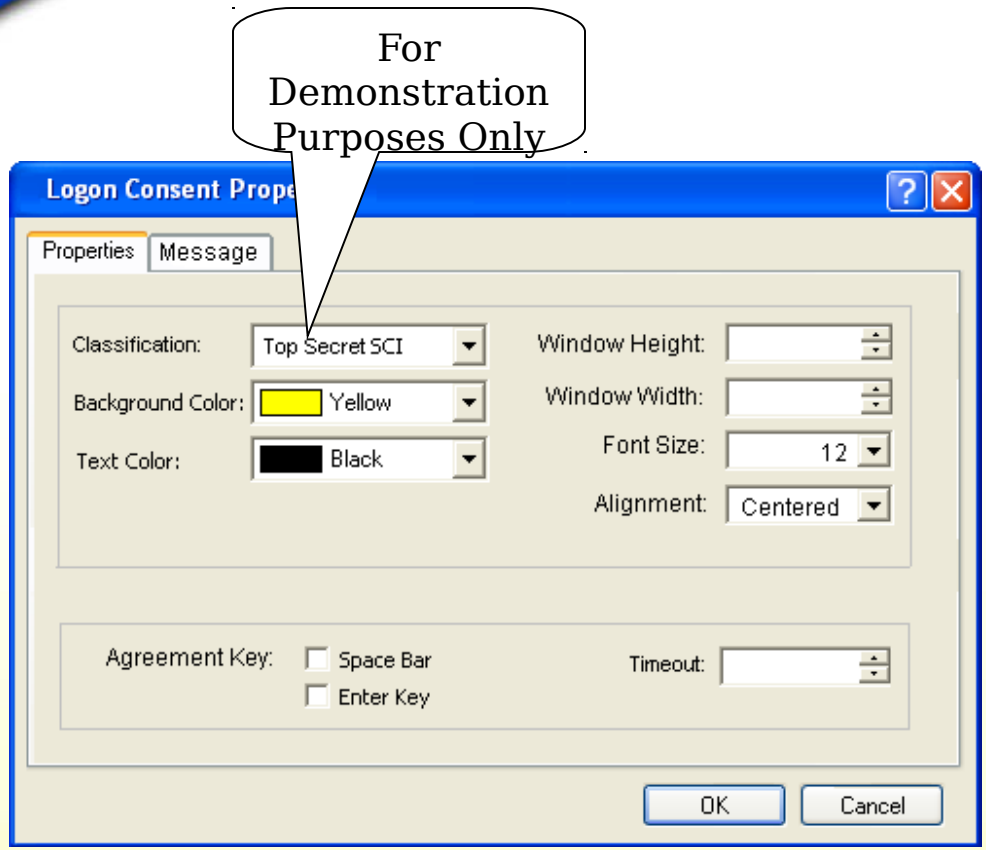


Logon Consent



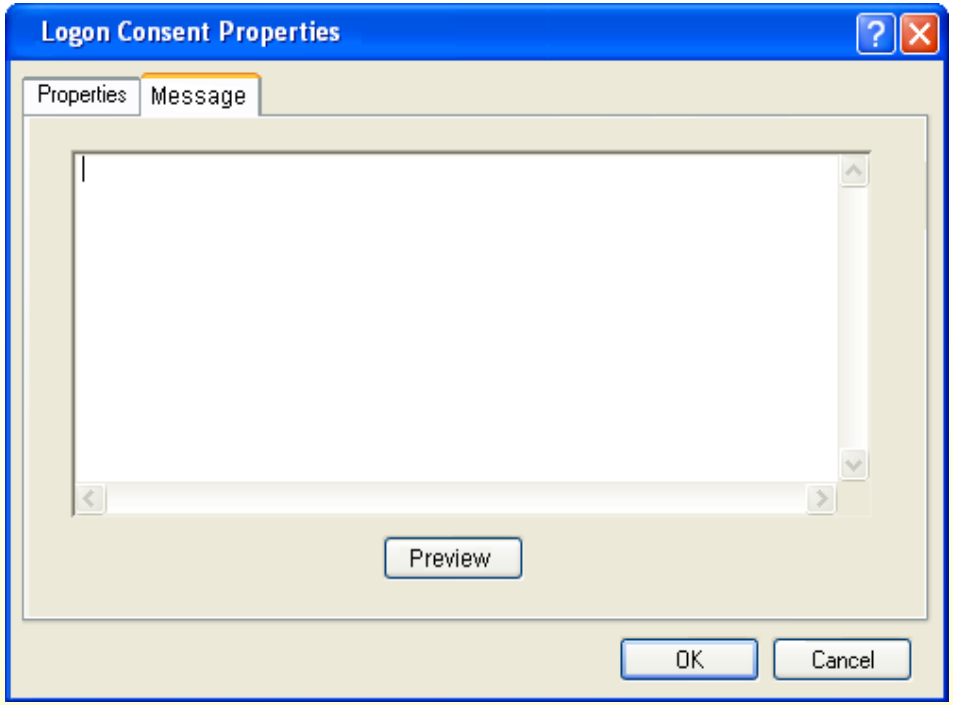
- Display a legal notice banner after the user is authenticated
- The user must agree to the banner before being granted access to the system
- If the user selects “Decline”, they will be returned to the Logon Screen
- If the user fails to select either “Accept” or “Decline” in a configurable amount of time, the banner will timeout and return the user to the Logon Screen
- The appearance of the Logon Screen is configurable to match the security classification of the workstation
- A scroll bar will appear if the text is longer than the displa

Logon Consent



- An administrator can set the Classification and windows size through the JMC

Logon Consent



- An administrator can create a custom message

Questions

Questions???

Security Banner

Purpose

This design specification provides a blueprint for the implementation of the JEDI 2.0 Windows Security Banner. The purpose of this implementation is to provide a configurable Security Banner in JEDI.

Current Functionality

The JEDI for Windows product does not currently provide Security Banner functionality.

Proposed Functionality

- The Security Banner should be configurable, (e.g. color, text, and ability to add machine name, etc). Example: “Admin UNCLASS Machine name“
- The Security Banner must also remain "on top" of any window
- Requirement for screen bannering at top and/or bottom of screen calling out the classification of the machine

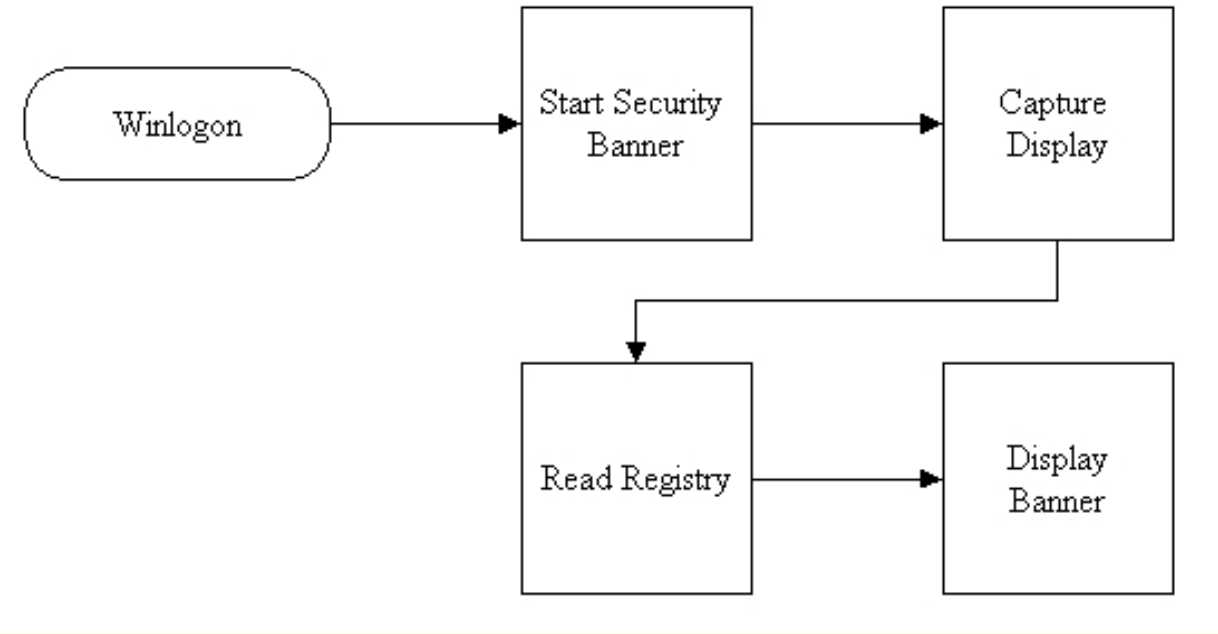
Security Banner (Cont.)

- Both background and text color should be configurable
- A trusted user should also be able to configure whether or not it appears at all
- Screen Markings – the default should be yellow background, black text
- The Security Banner should go completely across the screen at the top
- Entries for the configurable Security Banner settings should be added to the Windows Registry
- The Security Banner must be configurable through the use of an MMC snap-in GUI

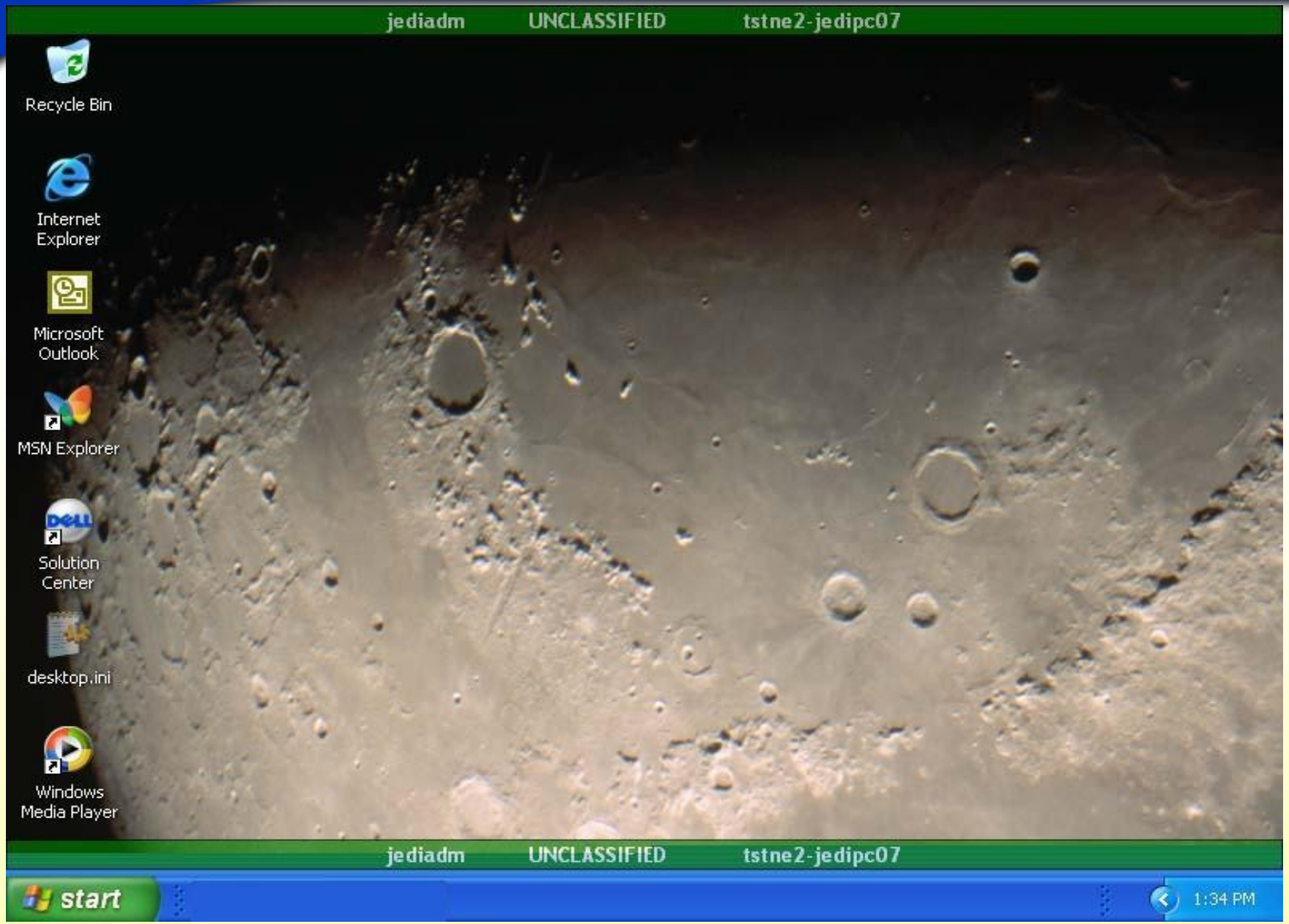
Security Banner (Cont.)

- For setting the security classification, the snap-in GUI will provide a list of standard classifications as well as the ability to enter an alternate classification
- The Security Banner will support Terminal Services
- All settings for the Security Banner will apply to all users
- The snap-in GUI will allow selection of background and foreground colors from a color palette
- The default security classification will be “Top Secret”
- Each classification will have a set of default colors associated with it

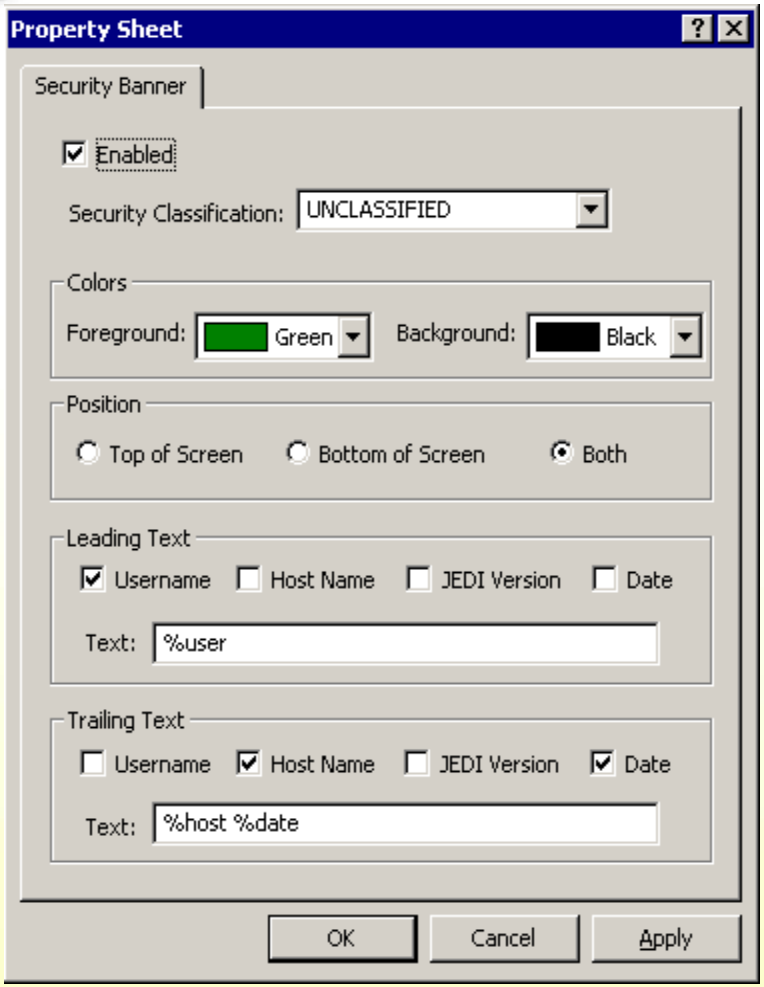
Security Banner Processing Diagram



Security Banner



Security Banner



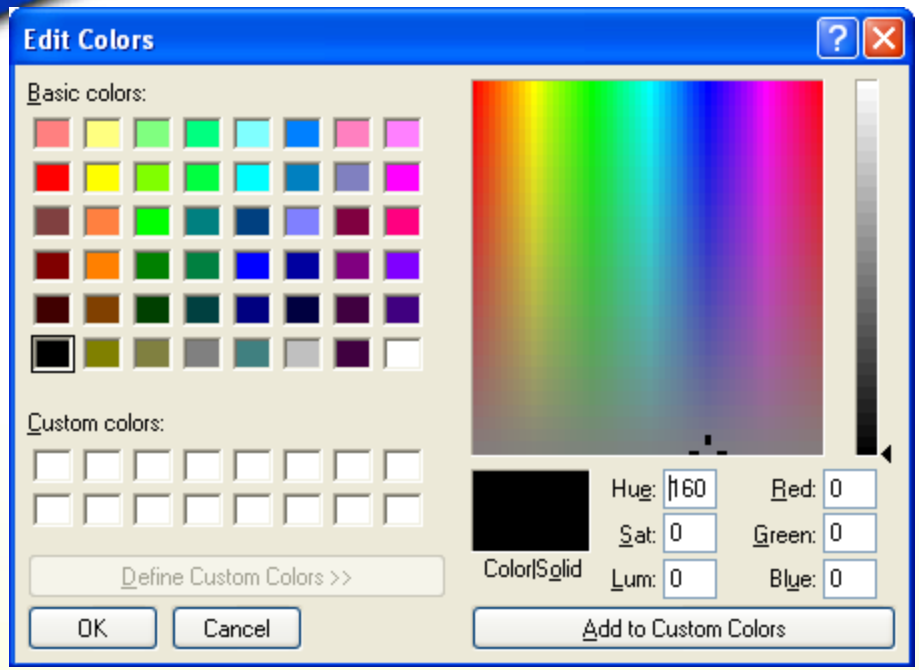
The default security classification list will include the following classifications.

- UNCLASSIFIED
- CONFIDENTIAL
- SECRET
- TOP SECRET
- TOP SECRET SCI

- Alternate security classifications may be entered by selecting the classification text in the Security Classification combo box and typing over the existing text

- Leading and Trailing text can be customized

Security Banner Color Classifications



- The list of colors in the Combo Box are the default system colors, and an option to choose a custom color

Questions

Questions???

FSD Support on Windows

Purpose

Full Service Directory support for Windows allows a site administrator the ability to specify any mandatory or optional FSD attribute for a user on a Windows network, as required for the Intelligence Community by the Chief Intelligence Officer.

Current Functionality

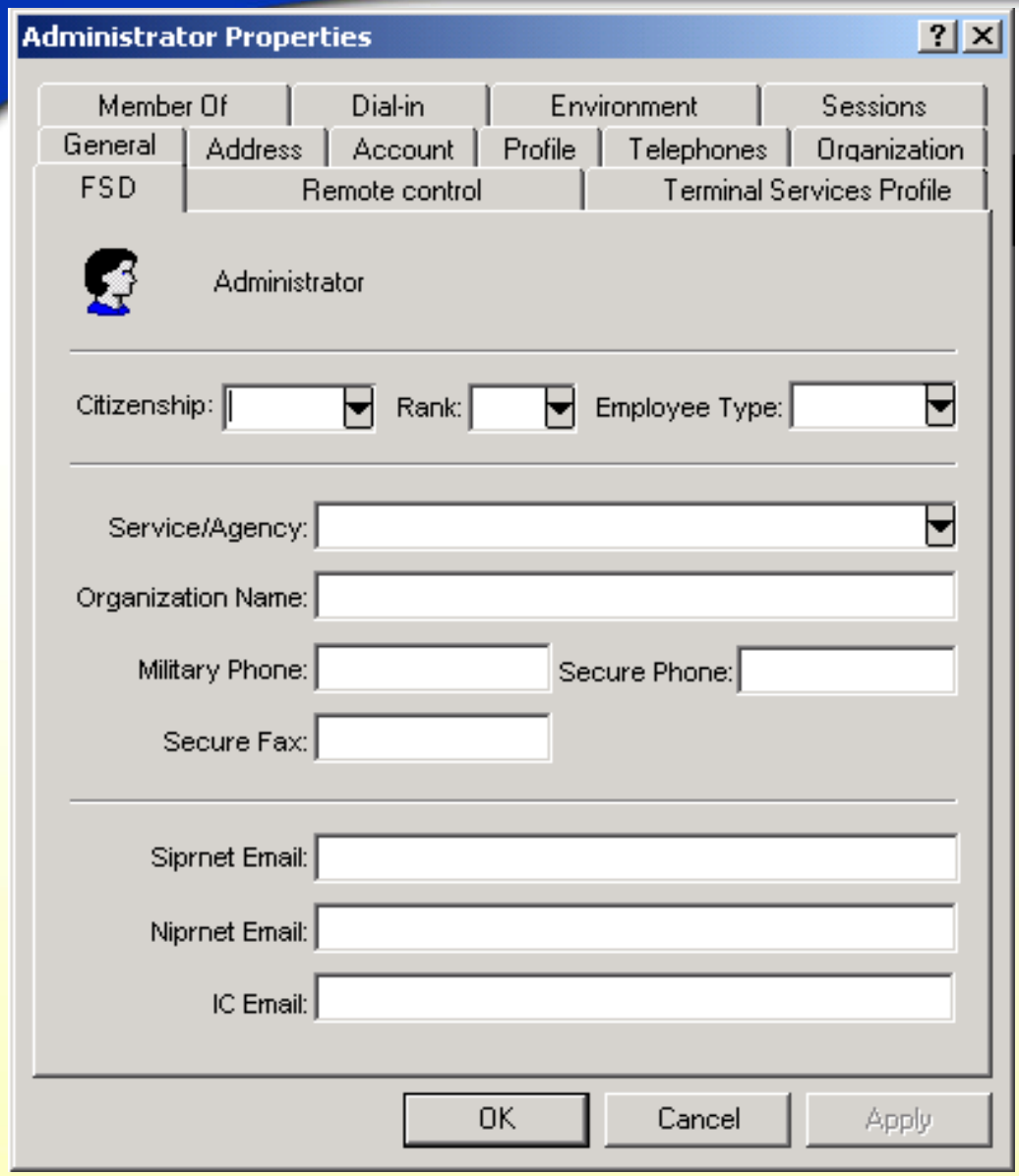
There is no FSD support available in the AFDI 1.2 version for Windows.

FSD Support on Windows (Cont.)

Proposed Functionality

- JEDI will extended of the Active Directory schema for users to contain the FSD attributes not currently available, as specified in the FSD Policy Guide
- The User Properties snap-in sheet, accessed from the Active Directory Users and Computers, will be modified to display an additional tab, “FSD”, which will contain a mix of text fields, drop-down menus and labels to allow the administrator to enter the desired values
  - Active Directory existing fields, such as “Last Name”, “Company Name”, etc., will be utilized as much as possible
- The default values, on the “FSD” tab, for a new user will be configurable during the installation of JEDI. These configuration settings will be stored in the registry
- The contents of the drop-down menus will also be configurable by modifying the registry manually

FSD GUI



- The FSD GUI is a tab attached to the Active Directory Primary snap-in Property sheet. It collects the desired settings for the various FSD attributes
- The FSD GUI will store the new attribute values for each user in the Windows Active Directory schema

FSD Design Notes

- The user account synchronization between UNIX users and Windows users will not be updated to include the FSD fields
- Windows users can still be updated from a JEDI 1.3 UNIX Administration machine, however, the FSD fields will not be affected by the update
- The JEDI documentation will detail how to send updates to the FSD PMO by making use of existing technology (ex. meta-directory)
- De-installing JEDI 2.0 will require leaving the extended schema in place. However, the FSD tabs will no longer be available on the User Properties snap-in

Questions on FSD

Questions???

Whitepaper (RIS) Notes

- Document RIS server setup
- Document installation of Windows 2000 Professional
- Document installation of Windows XP Professional
- Document installation of JEDI 2.0

Whitepaper (Sun ONE)

Advantages to using Sun ONE :

- Synchronizes users and users information between Sun ONE Directory server and Windows 2000 Active Directory (AD)
- Passwords
  - One password to remember
  - Change in one location
  - Password rules still enforced
  - No special applications needed
- Security
  - Network traffic is protected with SSL
  - All sensitive information is encrypted with 3DES encryption keys
  - Console provides system and product status
  - Audit and error logs available

Whitepaper (Sun ONE)

- Configuration
  - Ability to select a specific list of user entries for synchronization
  - Bi-directional synchronization of entries and attributes
- The only information found covered creating users and did not mention deleting users
- Only mentioned support for Windows 2000 and NT did not cover Windows 2003 or XP
- LDAP only
- Has not been released yet

Price

$3/entry quantity 1-250,000 entries for Identity Synchronization.

$1.25/entry quantity 1-999,999 entries for Directory Server 5.2.

Whitepaper (ISS)

- We are going to document the installation of System Scanner and Internet Scanner
- System Scanner is only for server OSes i.e. Windows NT, Windows 2000 and Unix
- Internet Scanner can be used for scanning non-server OSes i.e. Windows XP Professional
- As of now Windows 2003 is not supported for System Scanner. System Scanner plans to support Windows 2003 sometime in the first half of 2004
- System Scanner requires MSDE (Microsoft SQL server Desktop Environment) to be installed
- A system scan is run locally on each agent then the information is sent to the console host where the information is processed and the results are displayed
- There are different levels of scans. Using the highest scan level could fill up the audit logging directory and crash the host
- A key is required for installing System Scanner on a host that will have more than one agent (the ISS software counts itself as an agent)

DeviceLock

- Purchased by JEDI for the community
- DeviceLock for Windows NT/2000/XP and Windows Server 2003 gives network administrators control over which users can access what devices (floppies, USB, FireWire, infrared, serial and parallel ports, Magneto-Optical disks, CD-ROMs, ZIPs, etc.) on a local computer
- Once DeviceLock is installed, administrators can control access to floppies, CD-ROMs or any other device, depending on the time of day and day of the week
- It can protect network and local computers against viruses, trojans and other malicious programs often injected from removable disks
- Network administrators can also use DeviceLock to flush a storage device's buffers